

【特許請求の範囲】

【請求項1】 第1の情報処理装置を認証する第1の認証手段と、

第2の情報処理装置または第3の情報処理装置を認証する第2の認証手段と、

前記第1の情報処理装置からの、コンテンツおよび鍵の送信要求、並びに前記第2の情報処理装置を特定するデータまたは前記第3の情報処理装置を特定するデータの受信を制御する受信制御手段と、

前記第2の情報処理装置を特定する前記データを受信した場合、前記第2の情報処理装置に対応した手順で、前記第2の情報処理装置に前記コンテンツおよび前記鍵の送信要求を送信するとともに、前記第2の情報処理装置から前記コンテンツおよび前記鍵を受信し、前記第3の情報処理装置を特定する前記データを受信した場合、前記第3の情報処理装置に対応した手順で、前記第3の情報処理装置に前記コンテンツおよび前記鍵の送信要求を送信するとともに、前記第3の情報処理装置から前記コンテンツおよび前記鍵を受信するように通信を制御する通信制御手段と、

前記第1の情報処理装置への前記コンテンツおよび前記鍵の送信を制御する送信制御手段とを含むことを特徴とする情報提供装置。

【請求項2】 前記コンテンツの符号化方式および暗号化方式のうちの少なくとも一方を、所定の符号化方式または暗号化方式に変換する変換手段を更に含むことを特徴とする請求項1に記載の情報提供装置。

【請求項3】 第1の情報処理装置を認証する第1の認証ステップと、

第2の情報処理装置または第3の情報処理装置を認証する第2の認証ステップと、

前記第1の情報処理装置からの、コンテンツおよび鍵の送信要求、並びに前記第2の情報処理装置を特定するデータまたは前記第3の情報処理装置を特定するデータの受信を制御する受信制御ステップと、

前記第2の情報処理装置を特定する前記データを受信した場合、前記第2の情報処理装置に対応した手順で、前記第2の情報処理装置に前記コンテンツおよび前記鍵の送信要求を送信するとともに、前記第2の情報処理装置から前記コンテンツおよび前記鍵を受信し、前記第3の情報処理装置を特定する前記データを受信した場合、前記第3の情報処理装置に対応した手順で、前記第3の情報処理装置に前記コンテンツおよび前記鍵の送信要求を送信するとともに、前記第3の情報処理装置から前記コンテンツおよび前記鍵を受信するように通信を制御する通信制御ステップと、

前記第1の情報処理装置への前記コンテンツおよび前記鍵の送信を制御する送信制御ステップとを含むことを特徴とする情報提供方法。

【請求項4】 第1の情報処理装置を認証する第1の認

証ステップと、

第2の情報処理装置または第3の情報処理装置を認証する第2の認証ステップと、

前記第1の情報処理装置からの、コンテンツおよび鍵の送信要求、並びに前記第2の情報処理装置を特定するデータまたは前記第3の情報処理装置を特定するデータの受信を制御する受信制御ステップと、

前記第2の情報処理装置を特定する前記データを受信した場合、前記第2の情報処理装置に対応した手順で、前記第2の情報処理装置に前記コンテンツおよび前記鍵の送信要求を送信するとともに、前記第2の情報処理装置から前記コンテンツおよび前記鍵を受信し、前記第3の情報処理装置を特定する前記データを受信した場合、前記第3の情報処理装置に対応した手順で、前記第3の情報処理装置に前記コンテンツおよび前記鍵の送信要求を送信するとともに、前記第3の情報処理装置から前記コンテンツおよび前記鍵を受信するように通信を制御する通信制御ステップと、

前記第1の情報処理装置への前記コンテンツおよび前記鍵の送信を制御する送信制御ステップとを含むことを特徴とするコンピュータが読み取り可能なプログラムが格納されているプログラム格納媒体。

【請求項5】 第1の情報提供装置を認証する認証手段と、

前記第1の情報提供装置への、コンテンツおよび鍵の送信要求、並びに前記コンテンツおよび前記鍵を提供する第2の情報提供装置を特定するデータ、および前記コンテンツおよび前記鍵を提供する第3の情報提供装置を特定するデータのいずれかの送信を制御する送信制御手段と、

前記第2の情報提供装置または前記第3の情報提供装置から前記第1の情報提供装置が提供を受け、送信した前記コンテンツおよび前記鍵の受信を制御する受信制御手段とを含むことを特徴とする情報処理装置。

【請求項6】 第1の情報提供装置を認証する認証ステップと、

前記第1の情報提供装置への、コンテンツおよび鍵の送信要求、並びに前記コンテンツおよび前記鍵を提供する第2の情報提供装置を特定するデータ、および前記コンテンツおよび前記鍵を提供する第3の情報提供装置を特定するデータのいずれかの送信を制御する送信制御ステップと、

前記第2の情報提供装置または前記第3の情報提供装置から前記第1の情報提供装置が提供を受け、送信した前記コンテンツおよび前記鍵の受信を制御する受信制御ステップとを含むことを特徴とする情報処理方法。

【請求項7】 第1の情報提供装置を認証する認証ステップと、

前記第1の情報提供装置への、コンテンツおよび鍵の送信要求、並びに前記コンテンツおよび前記鍵を提供する

第2の情報提供装置を特定するデータ、および前記コンテンツおよび前記鍵を提供する第3の情報提供装置を特定するデータのいずれかの送信を制御する送信制御ステップと、

前記第2の情報提供装置または前記第3の情報提供装置から前記第1の情報提供装置が提供を受け、送信した前記コンテンツおよび前記鍵の受信を制御する受信制御ステップとを含むことを特徴とするコンピュータが読み取り可能なプログラムが格納されているプログラム格納媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、情報提供装置および方法、情報処理装置および方法、並びにプログラム格納媒体に関し、特に、コンテンツおよびコンテンツを復号する鍵を提供するか、または暗号化されているコンテンツを利用する情報提供装置および方法、情報処理装置および方法、並びにプログラム格納媒体に関する。

【0002】

【従来の技術】図1は、従来のデジタルデータ伝送システムの構成を示す図である。パーソナルコンピュータ1は、ローカルエリアネットワークまたはインターネットなどから構成される通信ネットワーク4に接続されている。パーソナルコンピュータ1は、コンテンツサーバ2-1若しくは2-2から受信した、またはCD(Compact Disc)から読み取った楽音のデータ(以下、コンテンツと称する)を、所定の圧縮の方式(例えば、ATRAC3(商標))に変換するとともにDES(Data Encryption Standard)などの暗号化方式で暗号化して記録する。

【0003】パーソナルコンピュータ1は、暗号化して記録しているコンテンツに対応して、コンテンツの利用条件を示す利用条件のデータを記録する。

【0004】利用条件のデータは、例えば、その利用条件のデータに対応するコンテンツを同時に利用することができるポータブルデバイス(Portable Device(PDとも称する))の台数(後述する、いわゆるチェックアウトできるPDの台数)を示す。利用条件のデータに示される数だけコンテンツをチェックアウトしたときでも、パーソナルコンピュータ1は、そのコンテンツを再生できる。

【0005】パーソナルコンピュータ1の表示操作指示プログラム11は、パーソナルコンピュータ1が記録しているコンテンツに関連するデータ(例えば、曲名、または利用条件など)を表示させるとともに、チェックアウトの指示などを入力して、SDMI(Secure Digital Music Initiative)の規格に準拠したソフトウェアモジュールであるLCM(Licensed Compliant Module)12にその指示に対応したチェックアウトなどの処理を実行させる。

【0006】パーソナルコンピュータ1のLCM12

は、コンテンツの不正な2次利用による著作権の侵害の防止を目的として、個々のコンテンツに対して著作権者が指定する利用条件でのみコンテンツを利用できるように制御を行うモジュール群から構成される。利用条件には、コンテンツの再生条件、コピー条件、移動条件、または蓄積条件などが含まれる。

【0007】LCM12は、パーソナルコンピュータ1に接続された機器が正当であるかの認証を行い、安全な方法でコンテンツの移動の処理などを実行する。コンテンツの移動の処理などに伴い、LCM12は、必要な鍵を生成して、鍵を管理し、コンテンツを暗号化し、または接続されている機器との通信を制御する。

【0008】また、LCM12は、装着されているポータブルメディア3の正当性をチェックして、サーバ5が指定した利用条件をコンテンツ(暗号化されている)に付加して、コンテンツを記録させる。

【0009】パーソナルコンピュータ1のLCM12は、暗号化して記録しているコンテンツを、コンテンツに関連するデータ(例えば、曲名、または利用条件など)と共に、接続されているポータブルデバイス2に供給するとともに、ポータブルデバイス2に供給したことに伴って、供給したコンテンツに対応する利用条件のデータを更新する(以下、チェックアウトと称する)。より詳細には、チェックアウトしたとき、パーソナルコンピュータ1が記録している、そのコンテンツに対応する利用条件のデータのチェックアウトできる回数は、1減らされる。チェックアウトできる回数が0のとき、対応するコンテンツは、チェックアウトすることができない。

【0010】ポータブルデバイス2は、パーソナルコンピュータ1から供給されたコンテンツ(すなわち、チェックアウトされたコンテンツ)を、コンテンツに関連するデータ(例えば、曲名、または利用条件など)と共に、装着されているポータブルメディア3に記憶させる。

【0011】ポータブルメディア3は、フラッシュメモリなどの記憶媒体をその内部に有し、ポータブルデバイス2に着脱可能に構成されている。

【0012】ポータブルデバイス2は、コンテンツに関連する利用条件のデータに基づいて、装着されているポータブルメディア3に記憶されているコンテンツを再生し、図示せぬヘッドフォンなどに出力する。

【0013】例えば、コンテンツに関連する利用条件のデータとして記憶されている、再生制限としての再生回数を超えて再生しようとしたとき、ポータブルデバイス2は、対応するコンテンツの再生を停止する。

【0014】使用者は、コンテンツを記憶したポータブルデバイス2をパーソナルコンピュータ1から取り外して、持ち歩き、ポータブルメディア3に記憶されているコンテンツを再生させて、コンテンツに対応する音楽な

どをヘッドフォンなどで聴くことができる。

【0015】ポータブルデバイス2がUSBケーブル等を介してパーソナルコンピュータ1に接続されたとき、ポータブルデバイス2とパーソナルコンピュータ1とは、相互認証の処理を実行する。この相互認証の処理は、チャレンジレスポンス方式の認証の処理である。チャレンジレスポンス方式とは、パーソナルコンピュータ1が生成するある値（チャレンジ）に対して、ポータブルデバイス2がパーソナルコンピュータ1と共有している秘密鍵を使用して生成した値（レスポンス）で応答する方式である。

【0016】サーバ5-1は、所定の方式で圧縮符号化され、暗号化されたコンテンツを蓄積して、パーソナルコンピュータ1からの要求に対応して蓄積しているコンテンツを配信する。サーバ5-1は、鍵サーバ21-1、コンテンツサーバ22-1、およびショップサーバ23-1の機能を有する。

【0017】鍵サーバ21-1は、コンテンツサーバ22-1がパーソナルコンピュータ1に供給したコンテンツを復号するためのコンテンツ鍵を蓄積し、パーソナルコンピュータ1の要求に対応して、コンテンツ鍵をパーソナルコンピュータ1に供給する。コンテンツ鍵の供給の前に、鍵サーバ21-1とパーソナルコンピュータ1とは、相互認証の処理を実行して、鍵サーバ21-1は、その相互認証の処理により共有された一時鍵でコンテンツ鍵を暗号化して、パーソナルコンピュータ1に送信する。パーソナルコンピュータ1は、受信したコンテンツ鍵を共有している一時鍵で復号する。

【0018】コンテンツサーバ22-1は、パーソナルコンピュータ1の要求に対応して、通信ネットワーク4を介して、パーソナルコンピュータ1に、コンテンツに対応する利用条件と共にコンテンツ（暗号化されている）を供給する。

【0019】ショップサーバ23-1は、コンテンツサーバ22-1が供給するコンテンツに関連するデジタルデータ（コンテンツの曲名、価格などを含むコンテンツの一覧などを含む）をパーソナルコンピュータ1に提供するとともに、パーソナルコンピュータ1からのコンテンツの購入の申し込みに対応して、そのコンテンツを供給するコンテンツサーバ22-1のURL（Uniform Resource Locator）、およびそのコンテンツを復号するコンテンツ鍵を供給する鍵サーバ21-1のURLなどをパーソナルコンピュータ1に供給する。

【0020】サーバ5-2は、所定の方式で圧縮符号化され、暗号化されたコンテンツを蓄積して、パーソナルコンピュータ1からの要求に対応して蓄積しているコンテンツを配信する。サーバ5-2は、鍵サーバ21-2、コンテンツサーバ22-2、およびショップサーバ23-2の機能を有する。

【0021】鍵サーバ21-2は、コンテンツサーバ2

2-2がパーソナルコンピュータ1に供給したコンテンツを復号するためのコンテンツ鍵を蓄積し、パーソナルコンピュータ1の要求に対応して、コンテンツ鍵をパーソナルコンピュータ1に供給する。コンテンツ鍵の供給の前に、鍵サーバ21-2とパーソナルコンピュータ1とは、相互認証の処理を実行して、鍵サーバ21-2は、その相互認証の処理により共有された一時鍵でコンテンツ鍵を暗号化して、パーソナルコンピュータ1に送信する。パーソナルコンピュータ1は、受信したコンテンツ鍵を共有している一時鍵で復号する。

【0022】コンテンツサーバ22-2は、パーソナルコンピュータ1の要求に対応して、通信ネットワーク4を介して、パーソナルコンピュータ1に、コンテンツに対応する利用条件と共にコンテンツ（暗号化されている）を供給する。

【0023】ショップサーバ23-2は、コンテンツサーバ22-2が供給するコンテンツに関連するデジタルデータ（コンテンツの曲名、価格などを含むコンテンツの一覧などを含む）をパーソナルコンピュータ1に提供するとともに、パーソナルコンピュータ1からのコンテンツの購入の申し込みに対応して、そのコンテンツを供給するコンテンツサーバ22-2のURL、およびそのコンテンツを復号するコンテンツ鍵を供給する鍵サーバ21-2のURLなどをパーソナルコンピュータ1に供給する。

【0024】以下、サーバ5-1およびサーバ5-2を個々に区別する必要がないとき、単に、サーバ5と称する。以下、鍵サーバ21-1および鍵サーバ21-2を個々に区別する必要がないとき、単に、鍵サーバ21と称する。以下、コンテンツサーバ22-1およびコンテンツサーバ22-2を個々に区別する必要がないとき、単に、コンテンツサーバ22と称する。以下、ショップサーバ23-1およびショップサーバ23-2を個々に区別する必要がないとき、単に、ショップサーバ23と称する。

【0025】次に、図2を参照して、従来のデジタルデータ伝送システムの機能の構成について説明する。パーソナルコンピュータ1は、表示操作指示プログラム11およびLCM12に加えて、IP（Internet Protocol）通信プログラム13、ISP（Internet Service Provider）接続プログラム14、およびPHS（Personal Handyphone System）/IMT（International Mobile Telecommunication System）通信プログラム15を実行する。

【0026】PHS/IMT通信プログラム15は、公衆回線網31を介して通信を行うためのプログラムである。ISP接続プログラム14は、ISP32と接続するためのプログラムである。IP通信プログラム13は、HTTP（Hypertext Transport Protocol）74およびWap（Wireless Access Protocol）75などの手

続を包含し、通信ネットワーク4を介して、鍵サーバ21、コンテンツサーバ22、またはショップサーバ23と通信するためのプログラムである。

【0027】LCM12は、ライセンス管理プログラム51、ダウンロードプログラム52-1、ダウンロードプログラム52-2、およびフォーマット管理プログラム53から構成されている。

【0028】ライセンス管理プログラム51は、コンテンツの利用条件に基づいたコンテンツの利用を管理するためのプログラムであり、利用条件管理プログラム61、CDリップングプログラム62、およびPD認証プログラム63から構成されている。

【0029】利用条件管理プログラム61は、コンテンツの利用条件に基づいて、パーソナルコンピュータ1が記録しているコンテンツのチェックアウトなどを許可するか、または禁止するかなどの管理を実行するとともに、コンテンツのチェックアウトなどに対応して利用条件のデータを更新する。CDリップングプログラム62は、パーソナルコンピュータ1に装着されたCDからコンテンツを読み出すとともに、読み出したコンテンツに対応する利用条件を生成する。

【0030】PD認証プログラム63は、パーソナルコンピュータ1に装着されているポータブルデバイス2を認証する。

【0031】ダウンロードプログラム52-1は、サーバ5-1からコンテンツおよびコンテンツ鍵をダウンロードするためのプログラムであり、鍵管理プログラム64、コンテンツ管理プログラム65、鍵情報受信プログラム66、およびコンテンツ情報受信プログラム67から構成されている。

【0032】鍵管理プログラム64は、鍵サーバ21-1の認証の処理を実行して、鍵サーバ21-1からコンテンツ鍵を受信して、コンテンツに対応させてコンテンツ鍵を管理する。鍵管理プログラム64は、サーバ認証プログラム71および受信プログラム72から構成される。

【0033】サーバ認証プログラム71は、後述する処理により、鍵サーバ21-1を認証する。受信プログラム72は、通信ネットワーク4を介して、鍵サーバ21-1からコンテンツ鍵を受信する。

【0034】コンテンツ管理プログラム65は、通信ネットワーク4を介して、コンテンツサーバ22-1からコンテンツの利用条件のデータとともにコンテンツを受信して、コンテンツの利用条件のデータとともにコンテンツを記録する。コンテンツ管理プログラム65の受信プログラム73は、コンテンツサーバ22-1からコンテンツの利用条件のデータおよびコンテンツを受信する。

【0035】鍵情報受信プログラム66は、ショップサーバ23-1から、所望のコンテンツに対応するコンテ

ンツ鍵を供給する鍵サーバ21-1を特定するURLを受信する。コンテンツ情報受信プログラム67は、ショップサーバ23-1から、使用者が所望するコンテンツを特定するコンテンツID、およびそのコンテンツを供給するコンテンツサーバ22-1を特定するURLを受信する。

【0036】ダウンロードプログラム52-2は、サーバ5-2からコンテンツおよびコンテンツ鍵をダウンロードするためのプログラムであり、ダウンロードプログラム52-1と同様の構成を有するので、その説明は省略する。

【0037】フォーマット管理プログラム53は、コンテンツサーバ22-1または22-2からダウンロードしたコンテンツの符号化方式および暗号化方式をそれぞれ所定の方式に変換するとともに、CDから読み出したコンテンツを所定の方式で符号化して暗号化する。フォーマット管理プログラム53は、システム識別プログラム68およびフォーマット変換プログラム69から構成されている。

【0038】システム識別プログラム68は、コンテンツのダウンロード先が、サーバ5-1であるか、サーバ5-2であるかのいずれかを識別するためのプログラムである。フォーマット変換プログラム69は、コンテンツの符号化方式および暗号化方式を変換する。

【0039】ポータブルデバイス2は、ライセンス管理プログラム81、鍵管理プログラム82、およびコンテンツ管理プログラム83を実行する。

【0040】ライセンス管理プログラム81は、コンテンツに対応する利用条件を基に、コンテンツの再生の回数などを管理する利用条件管理プログラム91、パーソナルコンピュータ1を認証するPC認証プログラム92、およびポータブルメディア3を認証するPM認証プログラム93から構成される。

【0041】鍵管理プログラム82は、パーソナルコンピュータ1から供給されたコンテンツ鍵を、ポータブルメディア3が予め記憶している保存用鍵で暗号化させ、ポータブルメディア3に記憶させて管理する。

【0042】コンテンツ管理プログラム83は、パーソナルコンピュータ1から供給されたコンテンツを、ポータブルメディア3に記憶させて管理する。

【0043】ポータブルメディア3は、ライセンス管理プログラム101、鍵管理プログラム102、およびコンテンツ管理プログラム103を実行する。

【0044】ライセンス管理プログラム101は、ポータブルデバイス2を認証するPD認証プログラム111を有し、コンテンツに対応する利用条件のデータを記憶して、利用条件のデータに基づいて、コンテンツの読み出し等を制御する。鍵管理プログラム102は、ポータブルデバイス2から供給されたコンテンツ鍵を、予め記憶している保存用鍵で暗号化して記憶し、管理する。コン

テンツ管理プログラム103は、ポータブルデバイス2から供給されたコンテンツを記憶して、管理する。

【0045】ショップサーバ23-1は、鍵情報送信プログラム121、コンテンツ情報送信プログラム122、閲覧プログラム123、およびIP通信プログラム124を実行する。

【0046】鍵情報送信プログラム121は、通信ネットワーク4を介して、パーソナルコンピュータ1に、パーソナルコンピュータ1の使用者が所望するコンテンツに対応するコンテンツ鍵を供給する鍵サーバ21-1のURLを送信する。

【0047】コンテンツ情報送信プログラム122は、通信ネットワーク4を介して、パーソナルコンピュータ1に、パーソナルコンピュータ1の使用者が所望するコンテンツを供給するコンテンツサーバ22-1のURLを送信する。

【0048】閲覧プログラム123は、コンテンツをパーソナルコンピュータ1の使用者に視聴させる視聴プログラム131、およびパーソナルコンピュータ1の使用者が所望のコンテンツを検索する検索プログラム132から構成されている。

【0049】IP通信プログラム124は、HTTP133およびWap134などの手続を包含し、通信ネットワーク4を介して、パーソナルコンピュータ1と通信するためのプログラムである。

【0050】鍵サーバ21-1は、認証プログラム151、鍵配信プログラム152、鍵保存プログラム153、鍵生成プログラム154、およびIP通信プログラム155を実行する。

【0051】認証プログラム151は、パーソナルコンピュータ1などを認証するプログラムである。鍵配信プログラム152は、認証されたパーソナルコンピュータ1に、鍵保存プログラム153が保存しているコンテンツ鍵を配信するプログラムである。鍵保存プログラム153は、鍵生成プログラム154により生成されたコンテンツ鍵を保存するプログラムである。鍵生成プログラム154は、コンテンツに対応させてコンテンツ鍵を生成するプログラムである。

【0052】IP通信プログラム155は、HTTP171およびWap172などの手続を包含し、通信ネットワーク4を介して、パーソナルコンピュータ1などと通信するためのプログラムである。

【0053】コンテンツサーバ22-1は、コンテンツ保存プログラム191、コンテンツ配信プログラム192、およびIP通信プログラム193を実行する。

【0054】コンテンツ保存プログラム191は、暗号化されているコンテンツをコンテンツIDと対応させて保存する。コンテンツ配信プログラム192は、パーソナルコンピュータ1から要求があったとき、コンテンツ保存プログラム191が保存している、コンテンツID

に対応するコンテンツをパーソナルコンピュータ1に配信する。

【0055】IP通信プログラム193は、HTTP201およびWap202などの手続を包含し、通信ネットワーク4を介して、パーソナルコンピュータ1と通信するためのプログラムである。

【0056】ショップサーバ23-2は、ショップサーバ23-1と同様の構成を有するので、その説明は省略する。鍵サーバ21-2は、鍵サーバ21-1と同様の構成を有するので、その説明は省略する。コンテンツサーバ22-2は、コンテンツサーバ22-1と同様の構成を有するのでその説明は省略する。

【0057】次に、パーソナルコンピュータ1がサーバ5-1からコンテンツをダウンロードして、ポータブルデバイス2にチェックアウトする従来の処理を図3および図4のフローチャートを参照して説明する。ステップS101において、パーソナルコンピュータ1のPHS/IMT通信プログラム15は、公衆回線網31と接続を確立する。ステップS201において、公衆回線網31の図示せぬ地上局などは、パーソナルコンピュータ1と接続を確立する。

【0058】ステップS102において、パーソナルコンピュータ1のISP接続プログラム14は、ISP32と接続を確立する。ステップS301において、ISP32は、パーソナルコンピュータ1と接続を確立する。

【0059】ステップS103において、パーソナルコンピュータ1のIP通信プログラム13は、ショップサーバ23とIP通信を確立する。ステップS401において、ショップサーバ23-1のIP通信プログラム124は、パーソナルコンピュータ1とIP通信を確立する。

【0060】ステップS402において、ショップサーバ23-1の閲覧プログラム123は、通信ネットワーク4を介して、パーソナルコンピュータ1に閲覧用(コンテンツの選択用)のデジタルデータを送信する。ステップS104において、パーソナルコンピュータ1の図示せぬブラウザプログラムは、デジタルデータに対応する画像またはテキストなどを表示し、使用者に閲覧させる。また、パーソナルコンピュータ1のブラウザプログラムは、コンテンツのストリーミング再生によりコンテンツを使用者に試聴させたり、または、キーワードによりコンテンツをショップサーバ23-1の閲覧プログラム123に検索させ、その結果を表示する。ステップS402およびステップS104の処理は、パーソナルコンピュータ1の使用者の要求に対応して、繰り返される。

【0061】ステップS105において、パーソナルコンピュータ1のブラウザプログラムは、購入依頼をショップサーバ23-1に送信する。ステップS403にお

いて、ショップサーバ23-1の閲覧プログラム123は、パーソナルコンピュータ1から送信された購入依頼を受信する。

【0062】ステップS404において、ショップサーバ23-1のコンテンツ情報送信プログラム122は、ステップS403の処理で受信した購入依頼に対応するコンテンツを配信するコンテンツサーバ22-1のURLおよびコンテンツを特定するためのコンテンツIDなどを含む、コンテンツ情報を通信ネットワーク4を介してパーソナルコンピュータ1に送信する。ステップS106において、パーソナルコンピュータ1のコンテンツ情報受信プログラム67は、ショップサーバ23-1が送信した、コンテンツ情報を受信する。

【0063】ステップS405において、ショップサーバ23-1の鍵情報送信プログラム121は、ステップS403の処理で受信した購入依頼に対応するコンテンツのコンテンツ鍵を配信する鍵サーバ21-1のURLなどの、鍵情報を通信ネットワーク4を介してパーソナルコンピュータ1に送信する。ステップS107において、パーソナルコンピュータ1の鍵情報受信プログラム66は、ショップサーバ23-1が送信した鍵情報を受信する。

【0064】ステップS108において、パーソナルコンピュータ1のIP通信プログラム13は、ステップS106の処理で取得したコンテンツ情報に含まれるコンテンツサーバ22-1のURLを基に、コンテンツサーバ22-1とIP通信を確立する。ステップS501において、コンテンツサーバ22-1のIP通信プログラム193は、パーソナルコンピュータ1とIP通信を確立する。

【0065】ステップS109において、パーソナルコンピュータ1のコンテンツ管理プログラム65は、ステップS106の処理で取得したコンテンツIDを、通信ネットワーク4を介して、コンテンツサーバ22-1に送信する。ステップS502において、コンテンツサーバ22-1は、パーソナルコンピュータ1が送信したコンテンツIDを受信する。ステップS503において、コンテンツサーバ22-1のコンテンツ配信プログラム192は、ステップS502で受信したコンテンツIDに対応するコンテンツ（暗号化されている）をコンテンツ保存プログラム191から読み出して、通信ネットワーク4を介して、パーソナルコンピュータ1に配信する。ステップS110において、パーソナルコンピュータ1のコンテンツ管理プログラム65の受信プログラム73は、コンテンツサーバ22-1が送信したコンテンツを受信する。

【0066】ステップS111において、パーソナルコンピュータ1のIP通信プログラム13は、ステップS107の処理で取得した鍵情報に含まれる鍵サーバ21-1のURLを基に、鍵サーバ21-1とIP通信を確

立する。ステップS601において、鍵サーバ21-1のIP通信プログラム155は、パーソナルコンピュータ1とIP通信を確立する。

【0067】ステップS112において、パーソナルコンピュータ1の鍵管理プログラム64のサーバ認証プログラム71は、鍵サーバ21-1を認証する。ステップS602において、鍵サーバ21-1の認証プログラム151は、パーソナルコンピュータ1を認証する。

【0068】鍵サーバ21-1には、マスター鍵KMSが予め記憶されており、パーソナルコンピュータ1には、個別鍵KPPとパーソナルコンピュータ1のIDが予め記憶されている。パーソナルコンピュータ1には、更に、マスター鍵KMPが予め記憶されており、鍵サーバ21-1にも鍵サーバ21-1のIDと個別鍵KPSが記憶されている。

【0069】鍵サーバ21-1は、パーソナルコンピュータ1から、パーソナルコンピュータ1のIDの供給を受け、そのIDと自分自身が有するマスター鍵KMSにハッシュ関数を適用して、パーソナルコンピュータ1の個別鍵KPPと同一の鍵を生成する。

【0070】パーソナルコンピュータ1は、鍵サーバ21-1から、鍵サーバ21-1のIDの供給を受け、そのIDと自分自身が有するマスター鍵KMPにハッシュ関数を適用して、鍵サーバ21-1の個別鍵KPSと同一の鍵を生成する。このようにすることで、パーソナルコンピュータ1と鍵サーバ21-1の両方に、共通の個別鍵が共有されることになる。これらの個別鍵を用いてさらに、一時鍵を生成する。

【0071】ステップS113において、パーソナルコンピュータ1の鍵管理プログラム64は、コンテンツIDを鍵サーバ21-1に送信する。ステップS603において、鍵サーバ21-1は、パーソナルコンピュータ1が送信した、コンテンツIDを受信する。ステップS604において、鍵サーバ21-1の鍵配信プログラム152は、鍵保存プログラム153がコンテンツIDと対応づけて保存しているコンテンツ鍵を読み出し、通信ネットワーク4を介して、そのコンテンツ鍵（一時鍵により暗号化されている）をパーソナルコンピュータ1に送信する。ステップS114において、パーソナルコンピュータ1の鍵管理プログラム64の受信プログラム72は、鍵サーバ21-1が送信したコンテンツ鍵を受信する。鍵管理プログラム64は、受信したコンテンツ鍵を一時鍵で復号する。

【0072】ステップS115において、パーソナルコンピュータ1のPHS/IMT通信プログラム15は、公衆回線網31との接続を切断する。ステップS202において、公衆回線網31の図示せぬ地上局などは、パーソナルコンピュータ1との接続を切断する。

【0073】ステップS116において、フォーマット管理プログラム53は、ステップS110の処理で受信

したコンテンツの符号化方式および暗号化方式を、それぞれ所定の方式に変換する。

【0074】パーソナルコンピュータ1の使用者が、表示操作指示プログラム11に対し、受信したコンテンツのチェックアウトを指示したとき、ステップS117以降の処理が実行される。

【0075】ステップS117において、パーソナルコンピュータ1のライセンス管理プログラム51のPD認証プログラム63は、ポータブルデバイス2を認証する。ステップS701において、ポータブルデバイス2のライセンス管理プログラム81のPC認証プログラム92は、パーソナルコンピュータ1を認証する。

【0076】ステップS117およびステップS701におけるパーソナルコンピュータ1とポータブルデバイス2との相互認証の処理は、チャレンジレスポンス方式の認証の処理であり、ステップS112およびステップS602における鍵サーバ21-1とパーソナルコンピュータ1との相互認証の処理に比較して、演算量が少ない。パーソナルコンピュータ1およびポータブルデバイス2は、それぞれ、同一の演算で、レスポンスから一時鍵を生成して、共有する。

【0077】ステップS118において、パーソナルコンピュータ1のコンテンツ管理プログラム65は、暗号化されているコンテンツをポータブルデバイス2に配信する。ステップS702において、ポータブルデバイス2のコンテンツ管理プログラム83は、パーソナルコンピュータ1が配信したコンテンツを受信して、ポータブルメディア3のコンテンツ管理プログラム103に供給する。ポータブルメディア3のコンテンツ管理プログラム103は、コンテンツを記憶する。

【0078】なお、ポータブルデバイス2とポータブルメディア3は、ポータブルデバイス2にポータブルメディア3が装着されたとき、相互認証する。

【0079】ステップS119において、パーソナルコンピュータ1の鍵管理プログラム64は、ポータブルデバイス2に、ステップS118で配信したコンテンツに対応するコンテンツ鍵（ポータブルデバイス2とポータブルメディア3とで共有する一時鍵で暗号化されている）を配信する。ステップS703において、ポータブルデバイス2の鍵管理プログラム82は、パーソナルコンピュータ1が配信したコンテンツ鍵を受信して、ポータブルメディア3の鍵管理プログラム102に供給する。ポータブルメディア3の鍵管理プログラム102は、コンテンツ鍵を一時鍵で復号して、コンテンツ鍵を記憶する。

【0080】次に、パーソナルコンピュータ1がサーバ5-2からコンテンツをダウンロードして、ポータブルデバイス2にチェックアウトする処理を図5および図6のフローチャートを参照して説明する。ステップS1101乃至ステップS1107の処理は、サーバ5-2、

並びにIP通信プログラム13、ISP接続プログラム14、PHS/IMT通信プログラム15、およびダウンロードプログラム52-2により実行され、それぞれ、ステップS101乃至ステップS107の処理と同様なので、その説明は省略する。

【0081】ステップS1108において、パーソナルコンピュータ1のIP通信プログラム13は、ステップS1107の処理で取得した鍵情報に含まれる鍵サーバ21-2のURLを基に、鍵サーバ21-2とIP通信を確立する。ステップS1601において、鍵サーバ21-2は、パーソナルコンピュータ1とIP通信を確立する。

【0082】ステップS1109において、パーソナルコンピュータ1のダウンロードプログラム52-2は、鍵サーバ21-2を認証する。ステップS1602において、鍵サーバ21-2は、パーソナルコンピュータ1を認証する。ステップS1109およびステップS1602の処理は、ステップS112およびステップS602の処理と同様の処理である。

【0083】ステップS1110において、パーソナルコンピュータ1のダウンロードプログラム52-2は、コンテンツIDを鍵サーバ21-2に送信する。ステップS1603において、鍵サーバ21-2は、パーソナルコンピュータ1が送信した、コンテンツIDを受信する。ステップS1604において、鍵サーバ21-2は、コンテンツIDと対応づけて保存しているコンテンツ鍵を読み出し、通信ネットワーク4を介して、そのコンテンツ鍵（一時鍵により暗号化されている）をパーソナルコンピュータ1に送信する。ステップS1111において、パーソナルコンピュータ1のダウンロードプログラム52-2は、鍵サーバ21-2が送信したコンテンツ鍵を受信する。ダウンロードプログラム52-2は、受信したコンテンツ鍵を一時鍵で復号する。

【0084】ステップS1112において、パーソナルコンピュータ1のIP通信プログラム13は、ステップS1106の処理で取得したコンテンツ情報に含まれるコンテンツサーバ22-2のURLを基に、コンテンツサーバ22-2とIP通信を確立する。ステップS1501において、コンテンツサーバ22-2は、パーソナルコンピュータ1とIP通信を確立する。

【0085】ステップS1113において、パーソナルコンピュータ1のダウンロードプログラム52-2は、ステップS1106の処理で取得したコンテンツIDを、通信ネットワーク4を介して、コンテンツサーバ22-2に送信する。ステップS1502において、コンテンツサーバ22-2は、パーソナルコンピュータ1が送信したコンテンツIDを受信する。ステップS1503において、コンテンツサーバ22-2は、ステップS1502で受信したコンテンツIDに対応するコンテンツ（暗号化されている）を読み出して、通信ネットワー

ク4を介して、パーソナルコンピュータ1に配信する。ステップS1114において、パーソナルコンピュータ1のダウンロードプログラム52-2は、コンテンツサーバ22-2が送信したコンテンツを受信する。

【0086】ステップS1115乃至ステップS1703の処理は、ステップS115乃至ステップS703の処理と同様なので、その説明は省略する。

【0087】

【発明が解決しようとする課題】以上のように、コンテンツおよびコンテンツ鍵を供給するサーバ5-1または5-2は、それぞれ、コンテンツおよびコンテンツ鍵を供給する手順が異なるので、サーバ5-1および5-2からのコンテンツの受信を所望する場合、サーバ5-1に対応するダウンロードプログラム52-1とサーバ5-2に対応するダウンロードプログラム52-2とが必要となる。

【0088】しかしながら、コンテンツを受信する装置の、演算能力が小さい、記憶容量が少ないなどの処理能力が小さい場合、コンテンツを受信する装置は、複数のダウンロードプログラムを記憶しておくことができず、ダウンロードプログラムを切り換えて実行することができない。

【0089】本発明はこのような状況に鑑みてなされたものであり、処理能力が小さい装置でも、異なる手順で供給されるコンテンツおよび鍵を受信することができるようにすることを目的とする。

【0090】

【課題を解決するための手段】請求項1に記載の情報提供装置は、第1の情報処理装置を認証する第1の認証手段と、第2の情報処理装置または第3の情報処理装置を認証する第2の認証手段と、第1の情報処理装置からの、コンテンツおよび鍵の送信要求、並びに第2の情報処理装置を特定するデータまたは第3の情報処理装置を特定するデータの受信を制御する受信制御手段と、第2の情報処理装置を特定するデータを受信した場合、第2の情報処理装置に対応した手順で、第2の情報処理装置にコンテンツおよび鍵の送信要求を送信するとともに、第2の情報処理装置からコンテンツおよび鍵を受信し、第3の情報処理装置を特定するデータを受信した場合、第3の情報処理装置に対応した手順で、第3の情報処理装置にコンテンツおよび鍵の送信要求を送信するとともに、第3の情報処理装置からコンテンツおよび鍵を受信するように通信を制御する通信制御手段と、第1の情報処理装置へのコンテンツおよび鍵の送信を制御する送信制御手段とを含むことを特徴とする。

【0091】情報提供装置は、コンテンツの符号化方式および暗号化方式のうちの少なくとも一方を、所定の符号化方式または暗号化方式に変換する変換手段を更に設けこたできる。

【0092】請求項3に記載の情報提供方法は、第1の

情報処理装置を認証する第1の認証ステップと、第2の情報処理装置または第3の情報処理装置を認証する第2の認証ステップと、第1の情報処理装置からの、コンテンツおよび鍵の送信要求、並びに第2の情報処理装置を特定するデータまたは第3の情報処理装置を特定するデータの受信を制御する受信制御ステップと、第2の情報処理装置を特定するデータを受信した場合、第2の情報処理装置に対応した手順で、第2の情報処理装置にコンテンツおよび鍵の送信要求を送信するとともに、第2の情報処理装置からコンテンツおよび鍵を受信し、第3の情報処理装置を特定するデータを受信した場合、第3の情報処理装置に対応した手順で、第3の情報処理装置にコンテンツおよび鍵の送信要求を送信するとともに、第3の情報処理装置からコンテンツおよび鍵を受信するように通信を制御する通信制御ステップと、第1の情報処理装置へのコンテンツおよび鍵の送信を制御する送信制御ステップとを含むことを特徴とする。

【0093】請求項4に記載のプログラム格納媒体のプログラムは、第1の情報処理装置を認証する第1の認証ステップと、第2の情報処理装置または第3の情報処理装置を認証する第2の認証ステップと、第1の情報処理装置からの、コンテンツおよび鍵の送信要求、並びに第2の情報処理装置を特定するデータまたは第3の情報処理装置を特定するデータの受信を制御する受信制御ステップと、第2の情報処理装置を特定するデータを受信した場合、第2の情報処理装置に対応した手順で、第2の情報処理装置にコンテンツおよび鍵の送信要求を送信するとともに、第2の情報処理装置からコンテンツおよび鍵を受信し、第3の情報処理装置を特定するデータを受信した場合、第3の情報処理装置に対応した手順で、第3の情報処理装置にコンテンツおよび鍵の送信要求を送信するとともに、第3の情報処理装置からコンテンツおよび鍵を受信するように通信を制御する通信制御ステップと、第1の情報処理装置へのコンテンツおよび鍵の送信を制御する送信制御ステップとを含むことを特徴とする。

【0094】請求項5に記載の情報処理装置は、第1の情報提供装置を認証する認証手段と、第1の情報提供装置への、コンテンツおよび鍵の送信要求、並びにコンテンツおよび鍵を提供する第2の情報提供装置を特定するデータ、およびコンテンツおよび鍵を提供する第3の情報提供装置を特定するデータのいずれかの送信を制御する送信制御手段と、第2の情報提供装置または第3の情報提供装置から第1の情報提供装置が提供を受け、送信したコンテンツおよび鍵の受信を制御する受信制御手段とを含むことを特徴とする。

【0095】請求項6に記載の情報処理方法は、第1の情報提供装置を認証する認証ステップと、第1の情報提供装置への、コンテンツおよび鍵の送信要求、並びにコンテンツおよび鍵を提供する第2の情報提供装置を特定

するデータ、およびコンテンツおよび鍵を提供する第3の情報提供装置を特定するデータのいずれかの送信を制御する送信制御ステップと、第2の情報提供装置または第3の情報提供装置から第1の情報提供装置が提供を受け、送信したコンテンツおよび鍵の受信を制御する受信制御ステップとを含むことを特徴とする。

【0096】請求項7に記載のプログラム格納媒体のプログラムは、第1の情報提供装置を認証する認証ステップと、第1の情報提供装置への、コンテンツおよび鍵の送信要求、並びにコンテンツおよび鍵を提供する第2の情報提供装置を特定するデータ、およびコンテンツおよび鍵を提供する第3の情報提供装置を特定するデータのいずれかの送信を制御する送信制御ステップと、第2の情報提供装置または第3の情報提供装置から第1の情報提供装置が提供を受け、送信したコンテンツおよび鍵の受信を制御する受信制御ステップとを含むことを特徴とする。

【0097】請求項1に記載の情報提供装置、請求項3に記載の情報提供方法、および請求項4に記載のプログラム格納媒体においては、第1の情報処理装置が認証され、第2の情報処理装置または第3の情報処理装置が認証され、第1の情報処理装置からの、コンテンツおよび鍵の送信要求、並びに第2の情報処理装置を特定するデータまたは第3の情報処理装置を特定するデータの受信が制御され、第2の情報処理装置を特定するデータを受信した場合、第2の情報処理装置に対応した手順で、第2の情報処理装置にコンテンツおよび鍵の送信要求を送信するとともに、第2の情報処理装置からコンテンツおよび鍵を受信し、第3の情報処理装置を特定するデータを受信した場合、第3の情報処理装置に対応した手順で、第3の情報処理装置にコンテンツおよび鍵の送信要求を送信するとともに、第3の情報処理装置からコンテンツおよび鍵を受信するように通信が制御され、第1の情報処理装置へのコンテンツおよび鍵の送信が制御される。

【0098】請求項5に記載の情報処理装置、請求項6に記載の情報処理方法、および請求項7に記載のプログラム格納媒体においては、第1の情報提供装置が認証され、第1の情報提供装置への、コンテンツおよび鍵の送信要求、並びにコンテンツおよび鍵を提供する第2の情報提供装置を特定するデータ、およびコンテンツおよび鍵を提供する第3の情報提供装置を特定するデータのいずれかの送信が制御され、第2の情報提供装置または第3の情報提供装置から第1の情報提供装置が提供を受け、送信したコンテンツおよび鍵の受信が制御される。

【0099】

【発明の実施の形態】図7は、本発明に係るデジタルデータ伝送システムの一実施の形態を示す図である。図1で説明した構成の場合と同一の部分には、図1の場合と同一の番号を付してあり、その説明は省略する。

【0100】電話機一体型端末機501は、ポータブルメディア3-1が装着可能に構成され、無線により、通信ネットワーク4に接続される。電話機一体型端末機501は、通信ネットワーク4を介して、コンテンツサーバ22-1または22-2から受信したコンテンツ（所定の方式で圧縮され、暗号化されている）を、利用条件のデータ等と共にダウンロードして、コンテンツおよびその利用条件データを装着されているポータブルメディア3-1に記憶させる。

【0101】電話機一体型端末機501は、コンテンツに関連する利用条件のデータに基づいて、装着されているポータブルメディア3-1に記憶されているコンテンツを再生し、図示せぬヘッドホンまたはスピーカなどに出力する。使用者は、電話機一体型端末機501を持ち歩きながら、所望の場所で所望のコンテンツをダウンロードして、そのコンテンツをポータブルメディア3-1に記憶させることができる。使用者は、電話機一体型端末機501に、ポータブルメディア3-1に記憶されているコンテンツを再生させて、コンテンツに対応する音楽などをヘッドホンなどで聴くことができる。

【0102】電話機一体型端末機501の表示操作指示プログラム511は、コンテンツに関連するデータ（例えば、曲名、または利用条件など）を表示させるとともに、ダウンロードの指示などを入力して、クライアント用LCM512にその指示に対応した処理を実行させる。電話機一体型端末機501のクライアント用LCM512は、代理サーバ503のサーバ用LCM514と協同して、利用条件データおよびコンテンツ等をダウンロードする一連の処理（後述する）を実行する。

【0103】電話機一体型端末機501のクライアント用LCM512は、コンテンツの不正な2次利用による著作権の侵害の防止を目的として、個々のコンテンツに対して著作権者が指定する利用条件でのみコンテンツを利用できるように制御を行うモジュール群から構成される。利用条件には、コンテンツの再生条件、コピー条件、移動条件、または蓄積条件などが含まれる。

【0104】クライアント用LCM512は、電話機一体型端末機501に装着されているポータブルメディア3-1が正当であるかの認証を行い、安全な方法でサーバ5が指定した利用条件のデータをコンテンツ（暗号化されている）に付加して、ポータブルメディア3-1にコンテンツを記録させる。コンテンツの移動の処理などに伴い、クライアント用LCM512は、必要な鍵を生成して、鍵を管理し、または接続されているポータブルメディア3-1との通信を制御する。

【0105】パーソナルコンピュータ502は、通信ネットワーク4に接続されている。パーソナルコンピュータ502は、コンテンツサーバ22-1若しくは22-2から受信した、またはCDから読み取ったコンテンツを、所定の圧縮の方式に変換するとともにDESなどの暗

号化方式で暗号化して記録する。パーソナルコンピュータ502は、暗号化して記録しているコンテンツに対応して、コンテンツの利用条件を示す利用条件のデータを記録する。

【0106】パーソナルコンピュータ502の表示操作指示プログラム11は、コンテンツに関連するデータ（例えば、曲名、または利用条件など）を表示させるとともに、ダウンロード、またはチェックアウトの指示などを入力して、LCM513にその指示に対応したダウンロード、またはチェックアウトなどの処理を実行させる。

【0107】パーソナルコンピュータ502のLCM513は、コンテンツの不正な2次利用による著作権の侵害の防止を目的として、個々のコンテンツに対して著作権者が指定する利用条件でのみコンテンツを利用できるように制御を行うモジュール群から構成される。利用条件には、コンテンツの再生条件、コピー条件、移動条件、または蓄積条件などが含まれる。

【0108】LCM513は、パーソナルコンピュータ502に接続されたポータブルデバイス2が正当であるかの認証を行い、安全な方法でコンテンツの移動の処理などを実行する。コンテンツの移動の処理などに伴い、LCM513は、必要な鍵を生成して、鍵を管理し、コンテンツを暗号化し、または接続されている機器との通信を制御する。

【0109】また、LCM513は、ポータブルデバイス2の正当性をチェックする。ポータブルデバイス2は、ポータブルメディア3-2が装着されたとき、ポータブルメディア3-2の正当性をチェックする。ポータブルデバイス2およびポータブルメディア3-2が正当である場合、LCM513は、サーバ5が指定した利用条件のデータをコンテンツ（暗号化されている）に付加して、ポータブルメディア3-2にコンテンツをチェックアウトする。ポータブルデバイス2は、パーソナルコンピュータ502からチェックアウトされたコンテンツを、コンテンツに関連するデータと共に、装着されているポータブルメディア3-2に記憶させる。

【0110】パーソナルコンピュータ502のLCM513は、暗号化して記録しているコンテンツを、接続されているポータブルデバイス2にチェックアウトする。ポータブルデバイス2は、パーソナルコンピュータ502からチェックアウトされたコンテンツを、コンテンツに関連するデータと共に、装着されているポータブルメディア3-2に記憶させる。

【0111】代理サーバ503を利用できるとき、パーソナルコンピュータ502のPC用LCM521（LCM513の一部または全部の機能から構成される）は、代理サーバ503のサーバ用LCM514と協同して、利用条件データおよびコンテンツ等をダウンロードする一連の処理を実行する。

【0112】代理サーバ503を利用できないとき、パーソナルコンピュータ502のLCM513は、LCM12と同様の鍵サーバ21-1または21-2との認証の処理等を実行して、利用条件データおよびコンテンツ等をダウンロードする。

【0113】代理サーバ503は、サーバ用LCM514を実行して、相互認証した電話機一体型端末機501または相互認証したパーソナルコンピュータ502の要求に対応して、鍵サーバ21-1または21-2との認証の処理を実行する。代理サーバ503は、鍵サーバ21-1または21-2との相互認証の処理の後、鍵サーバ21-1または21-2からコンテンツ鍵を受信して、受信したコンテンツ鍵を電話機一体型端末機501またはパーソナルコンピュータ502に供給する。代理サーバ503は、コンテンツサーバ22-1または22-2からコンテンツを受信して、受信したコンテンツを電話機一体型端末機501またはパーソナルコンピュータ502に供給する。

【0114】代理サーバ503は、サーバ5-1からコンテンツおよびコンテンツ鍵をダウンロードするとき、サーバ5-1からコンテンツを受信した後、コンテンツ鍵を受信する。代理サーバ503は、サーバ5-2からコンテンツおよびコンテンツ鍵をダウンロードするとき、コンテンツ鍵を受信した後、コンテンツを受信する。

【0115】代理サーバ503は、サーバ5-1からコンテンツおよびコンテンツ鍵をダウンロードしたときも、サーバ5-2からコンテンツおよびコンテンツ鍵をダウンロードしたときも、いずれの場合も、同一の手順（例えば、コンテンツ鍵を送信してから、コンテンツを送信する）で、電話機一体型端末機501またはパーソナルコンピュータ502にコンテンツおよびコンテンツ鍵を供給する。

【0116】電話機一体型端末機501またはパーソナルコンピュータ502は、代理サーバ503を介して、サーバ5-1または5-2からコンテンツおよびコンテンツ鍵をダウンロードすることにより、同一の手順でコンテンツおよびコンテンツ鍵を受信することができる。

【0117】図8は、電話機一体型端末機501の構成を説明する図である。CPU（Central Processing Unit）601は、ROM（Read-only Memory）602またはRAM（Random-Access Memory）603に格納されている各種プログラムを実際に実行する。ROM602は、EEPROM（Electrically Erasable Programmable Read-Only Memory）またはフラッシュメモリなどで構成され、一般的には、CPU601が使用するプログラムや演算用のパラメータのうちの基本的に固定のデータを格納する。RAM603は、SRAM（Static RAM）などで構成され、CPU601の実行において使用するプログラムや、その実行において適宜変化するパラメータを格納する。

【0118】入力部605は、入力キーまたはマイクロフォンなどで構成され、CPU601に各種の指令を入力するとき、または音声などを入力するとき、使用者により操作される。表示部606は、液晶表示装置などから成り、各種情報をテキストやイメージで表示する。

【0119】音声再生部607は、通信部608から供給された通話相手の音声のデータ、またはインターフェース609から供給されたポータブルメディア3-1に記憶されているコンテンツを再生して、音声を出力する。

【0120】通信部608は、公衆回線網31と接続し、CPU601から供給されたデータ（例えば、コンテンツの送信要求など）または入力部605から供給された使用者の音声のデータを、所定の方式のケットに格納して、公衆回線網31を介して、送信する。また、通信部608は、公衆回線網31を介して、受信したケットに格納されているデータ（例えば、コンテンツなど）または通話相手の音声のデータをCPU601、RAM603、音声再生部607、またはインターフェース609に出力する。

【0121】インターフェース609は、CPU601、RAM603、または通信部608から供給されたデータを装着されているポータブルメディア3-1に記憶させるとともに、装着されているポータブルメディア3-1からコンテンツなどのデータを読み出して、CPU601、RAM603、または音声再生部607に供給する。

【0122】インターフェース610は、外付けのドライブ631が接続される。ドライブ631は、装着されている磁気ディスク641、光ディスク642、(CD-ROMを含む)、光磁気ディスク643、または半導体メモリ644に記録されているデータまたはプログラムを読み出して、そのデータまたはプログラムを、インターフェース610、およびバス604を介して接続されているROM602またはRAM603に供給する。

【0123】CPU601乃至インターフェース610は、バス604により相互に接続されている。

【0124】図9は、代理サーバ503の構成を説明する図である。CPU651は、各種アプリケーションプログラム（詳細については後述する）や、OS (Operating System)を実際に行う。ROM652は、一般的には、CPU651が使用するプログラムや演算用のパラメータのうちの基本的に固定のデータを格納する。RAM653は、CPU651の実行において使用するプログラムや、その実行において適宜変化するパラメータを格納する。これらはCPUバスなどから構成されるホストバス654により相互に接続されている。

【0125】ホストバス654は、ブリッジ655を介して、PCI(Peripheral Component Interconnect/Interface)バスなどの外部バス656に接続されている。

【0126】キーボード658は、CPU651に各種の

指令を入力するとき、使用者により操作される。ポインティングデバイス659は、ディスプレイ660の画面上のポイントの指示や選択を行うとき、使用者により操作される。ディスプレイ660は、液晶表示装置またはCRT (Cathode Ray Tube) などから成り、各種情報をテキストやイメージで表示する。HDD (Hard Disk Drive) 661は、ハードディスクを駆動し、それらにCPU651によって実行するプログラムや情報を記録または再生させる。

【0127】ドライブ662は、装着されている磁気ディスク681、光ディスク682、光磁気ディスク683、または半導体メモリ684に記録されているデータまたはプログラムを読み出して、そのデータまたはプログラムを、インターフェース657、外部バス656、ブリッジ655、およびホストバス654を介して接続されているRAM653に供給する。

【0128】これらのキーボード658乃至ドライブ662は、インターフェース657に接続されており、インターフェース657は、外部バス656、ブリッジ655、およびホストバス654を介してCPU651に接続されている。

【0129】通信部663は、通信ネットワーク4が接続され、CPU651、またはHDD661から供給されたデータ（例えば、コンテンツ鍵など）を、所定の方式のケットに格納して、通信ネットワーク4を介して、送信するとともに、通信ネットワーク4を介して、受信したケットに格納されているデータ（例えば、コンテンツIDなど）をCPU651、RAM653、またはHDD661に出力する。

【0130】通信部663は、外部バス656、ブリッジ655、およびホストバス654を介してCPU651に接続されている。

【0131】次に、図10を参照して、本願のデジタルデータ伝送システムの機能の構成について説明する。図2で説明した構成の場合と同一の部分には、図2の場合と同一の番号を付してあり、その説明は省略する。

【0132】電話機一体型端末機501は、表示操作指示プログラム511、クライアント用LCM512、IP通信プログラム701、ISP接続プログラム702、およびPHS/IMT通信プログラム703を実行する。

【0133】PHS/IMT通信プログラム703は、公衆回線網31を介して通信を行うためのプログラムである。ISP接続プログラム702は、ISP32と接続するためのプログラムである。IP通信プログラム701は、HTTP741およびWap742などの手続を包含し、通信ネットワーク4を介して、鍵サーバ21-1、コンテンツサーバ22-1、ショップサーバ23-1、鍵サーバ21-2、コンテンツサーバ22-2、ショップサーバ23-2、または代理サーバ503など

と通信するためのプログラムである。

【0134】クライアント用LCM512は、ライセンス管理プログラム711、ダウンロードプログラム712、およびフォーマット管理プログラム713などから構成されている。

【0135】ライセンス管理プログラム711は、コンテンツの利用条件に基づいたコンテンツの利用を管理するためのプログラムであり、利用条件管理プログラム721、サーバ認証プログラム722、およびPM認証プログラム723などから構成されている。

【0136】利用条件管理プログラム721は、コンテンツの利用条件に基づいて、ポータブルメディア3-1が記憶しているコンテンツの再生などを許可するか、または禁止するかなどの管理を実行するとともに、ポータブルメディア3-1が記憶しているコンテンツの再生などに対応して、ポータブルメディア3-1に、ポータブルメディア3-1が記憶している利用条件のデータを更新させる。サーバ認証プログラム722は、通信ネットワーク4を介して、代理サーバ503を認証する。PM認証プログラム723は、ポータブルメディア3-1が電話機一体型端末機501に装着されたとき、ポータブルメディア3-1を認証する。

【0137】ダウンロードプログラム712は、鍵管理プログラム724、コンテンツ管理プログラム725、鍵情報受信プログラム726、およびコンテンツ情報受信プログラム727などから構成されている。

【0138】鍵管理プログラム724は、代理サーバ503からコンテンツ鍵を受信して、コンテンツに対応させて、コンテンツ鍵をポータブルメディア3-1に記憶させて、管理する。鍵管理プログラム724は、代理サーバ503からコンテンツ鍵を受信する受信プログラム731などを含む。

【0139】コンテンツ管理プログラム725は、代理サーバ503からコンテンツの利用条件とともにコンテンツ（暗号化されている）を受信して、コンテンツの利用条件とともにコンテンツをポータブルメディア3-1に記憶させる。コンテンツ管理プログラム725の受信プログラム732は、代理サーバ503からコンテンツの利用条件およびコンテンツを受信する。

【0140】鍵情報受信プログラム726は、ショップサーバ23-1または23-2から、コンテンツに対応するコンテンツ鍵を供給する鍵サーバ21-1または21-2を特定するURLを受信する。コンテンツ情報受信プログラム727は、ショップサーバ23-1または23-2から、所望のコンテンツを特定するコンテンツID、および所望のコンテンツを供給するコンテンツサーバ22-1または22-2を特定するURLを受信する。

【0141】フォーマット管理プログラム713は、代理サーバ503を介して、コンテンツサーバ22-1ま

たは22-2からダウンロードしたコンテンツの符号化方式および暗号化方式をそれぞれ所定の方式に変換する。フォーマット管理プログラム713は、システム識別プログラム728およびフォーマット変換プログラム729などから構成されている。

【0142】システム識別プログラム728は、コンテンツのダウンロード先が、サーバ5-1であるか、サーバ5-2であるかのいずれかを識別するためのプログラムである。フォーマット変換プログラム729は、コンテンツの符号化方式および暗号化方式を変換する。

【0143】次に、代理サーバ503の構成について説明する。代理サーバ503は、サーバ用LCM514、およびIP通信プログラム751を実行する。

【0144】サーバ用LCM514は、ライセンス管理プログラム761、およびシーケンス管理プログラム762などを含む。

【0145】ライセンス管理プログラム761は、更に、鍵サーバ21-1または21-2を認証するサーバ認証プログラム781、および電話機一体型端末機501を認証するPD認証プログラム782などを含む。

【0146】シーケンス管理プログラム762は、鍵管理プログラム771、コンテンツ管理プログラム772、およびシステム識別プログラム773などを含む。

【0147】鍵管理プログラム771は、更に、通信ネットワーク4を介して、鍵サーバ21-1または21-2からコンテンツ鍵を受信する鍵受信プログラム783、および通信ネットワーク4を介して、受信したコンテンツ鍵を電話機一体型端末機501に配信する鍵配信プログラム784などを含む。

【0148】コンテンツ管理プログラム772は、更に、通信ネットワーク4を介して、コンテンツサーバ22-1または22-2からコンテンツを受信するコンテンツ受信プログラム785、および通信ネットワーク4を介して、受信したコンテンツを電話機一体型端末機501に配信するコンテンツ配信プログラム786などを含む。

【0149】システム識別プログラム773は、電話機一体型端末機501から供給されたコンテンツIDを基に、コンテンツのダウンロード先が、サーバ5-1であるか、サーバ5-2であるかのいずれかを識別するためのプログラムである。

【0150】IP通信プログラム751は、HTTP787およびWap788などの手続を包含し、通信ネットワーク4を介して、サーバ5-1若しくは5-2、または電話機一体型端末機501と通信するためのプログラムである。

【0151】次に、電話機一体型端末機501がサーバ5-1からコンテンツをダウンロードする処理を図11および図12のフローチャートを参照して説明する。ステップS2101において、電話機一体型端末機501

のPHS/IMT通信プログラム703は、公衆回線網31と接続を確立する。ステップS2201において、公衆回線網31の図示せぬ地上局などは、電話機一体型端末機501と接続を確立する。

【0152】ステップS2102において、電話機一体型端末機501のISP接続プログラム702は、電話機一体型端末機501と公衆回線網31との接続を介して、ISP32と接続を確立する。ステップS2301において、ISP32は、電話機一体型端末機501と公衆回線網31との接続を介して、電話機一体型端末機501と接続を確立する。

【0153】以降の電話機一体型端末機501と、鍵サーバ21-1、コンテンツサーバ22-1、ショッピングサーバ23-1、または代理サーバ503との処理は、電話機一体型端末機501とISP32との接続を介して実行される。

【0154】ステップS2103において、電話機一体型端末機501のIP通信プログラム701は、ショッピングサーバ23-1とIP通信を確立する。ステップS2401において、ショッピングサーバ23-1のIP通信プログラム124は、電話機一体型端末機501とIP通信を確立する。

【0155】ステップS2402において、ショッピングサーバ23-1の閲覧プログラム123は、通信ネットワーク4を介して、電話機一体型端末機501に閲覧用（コンテンツの選択用）のデジタルデータを送信する。ステップS2104において、電話機一体型端末機501の図示せぬブラウザプログラムは、受信したデジタルデータに対応するテキストまたは画像を表示部606に表示させ、使用者に閲覧させる。また、電話機一体型端末機501のブラウザプログラムは、コンテンツのストリーミング再生により、コンテンツを音声再生部607に再生させて、使用者に試聴させたり、または、キーワードにより所望のコンテンツをショッピングサーバ23-1の閲覧プログラム123に検索させ、その結果を表示部606に表示させる。

【0156】ステップS2402およびステップS2104の処理は、電話機一体型端末機501の使用者の要求に対応して、例えば、使用者が購入するコンテンツを決定するまで繰り返される。

【0157】ステップS2105において、電話機一体型端末機501のブラウザプログラムは、通信ネットワーク4を介して、購入依頼をショッピングサーバ23-1に送信する。ステップS2403において、ショッピングサーバ23-1の閲覧プログラム123は、電話機一体型端末機501から送信された購入依頼を受信する。

【0158】ステップS2404において、ショッピングサーバ23-1のコンテンツ情報送信プログラム122は、ステップS2403の処理で受信した購入依頼に対応して、コンテンツを配信するコンテンツサーバ22-

1のURL、およびコンテンツを特定するためのコンテンツIDなどを含む、コンテンツ情報を、通信ネットワーク4を介して、電話機一体型端末機501に送信する。ステップS2106において、電話機一体型端末機501のコンテンツ情報受信プログラム727は、ショッピングサーバ23-1が送信した、コンテンツ情報を受信する。

【0159】ステップS2405において、ショッピングサーバ23-1の鍵情報送信プログラム121は、ステップS2403の処理で受信した購入依頼に対応するコンテンツのコンテンツ鍵を配信する鍵サーバ21-1のURLなどの、鍵情報を通信ネットワーク4を介して、電話機一体型端末機501に送信する。ステップS2107において、電話機一体型端末機501の鍵情報受信プログラム726は、ショッピングサーバ23-1が送信した、鍵情報を受信する。

【0160】ステップS2108において、電話機一体型端末機501のIP通信プログラム701は、予め記録している代理サーバ503のURLを基に、代理サーバ503とIP通信を確立する。ステップS2501において、代理サーバ503のIP通信プログラム751は、電話機一体型端末機501とIP通信を確立する。

【0161】ステップS2109において、電話機一体型端末機501のライセンス管理プログラム711のサーバ認証プログラム722は、代理サーバ503を認証する。ステップS2502において、代理サーバ503のライセンス管理プログラム761のPD認証プログラム782は、電話機一体型端末機501を認証する。

【0162】ステップS2109およびステップS2502における電話機一体型端末機501と代理サーバ503との相互認証の処理は、チャレンジレスポンス方式の認証の処理であり、ステップS112およびステップS602における鍵サーバ21-1とパーソナルコンピュータ1との相互認証の処理に比較して、演算量が少なく、少ない演算能力、または記憶容量でも、迅速に実行することができる。電話機一体型端末機501および代理サーバ503は、それぞれ、同一の演算で、レスポンスから一時鍵を生成して、共有する。

【0163】ステップS2109およびステップS2502における認証の処理に失敗したとき（認証の相手が正当でないと判定されたとき）、電話機一体型端末機501がコンテンツをダウンロードする処理は、コンテンツをダウンロードしないで、終了する。

【0164】ステップS2110において、電話機一体型端末機501のコンテンツ管理プログラム725は、コンテンツIDを代理サーバ503に送信する。ステップS2503において、代理サーバ503は、電話機一体型端末機501が送信したコンテンツIDを受信する。ステップS2111において、電話機一体型端末機501の鍵管理プログラム724は、ステップS210

7の処理で受信した鍵情報を代理サーバ503に送信する。ステップS2504において、代理サーバ503は、電話機一体型端末機501が送信した、鍵情報を受信する。

【0165】ステップS2505において、代理サーバ503のシステム識別プログラム773は、ステップS2503の処理で受信したコンテンツIDを基に、コンテンツおよびコンテンツ鍵のダウンロード先が、サーバ5-1であることを識別する。

【0166】なお、ステップS2110において、電話機一体型端末機501は、コンテンツIDと共にコンテンツサーバ22-1のURLを送信して、ステップS2503において、代理サーバ503は、コンテンツIDと共にコンテンツサーバ22-1のURLを受信するようにしてもよい。

【0167】ステップS2506において、代理サーバ503のIP通信プログラム751は、ステップS2505の処理の識別の結果を基に、コンテンツサーバ22-1とIP通信を確立する。ステップS2601において、コンテンツサーバ22-1のIP通信プログラム193は、代理サーバ503とIP通信を確立する。

【0168】ステップS2507において、代理サーバ503のコンテンツ管理プログラム772は、ステップS2503の処理で取得したコンテンツIDを、通信ネットワーク4を介して、コンテンツサーバ22-1に送信する。ステップS2602において、コンテンツサーバ22-1は、代理サーバ503が送信したコンテンツIDを受信する。ステップS2603において、コンテンツサーバ22-1のコンテンツ配信プログラム192は、ステップS2602で受信したコンテンツIDに対応するコンテンツ（暗号化されている）を、コンテンツ保存プログラム191から読み出して、通信ネットワーク4を介して、代理サーバ503に配信する。

【0169】ステップS2508において、代理サーバ503のコンテンツ管理プログラム772の受信プログラム785は、コンテンツサーバ22-1が送信したコンテンツを受信する。

【0170】ステップS2509において、代理サーバ503のIP通信プログラム751は、ステップS2505の処理の識別の結果を基に、鍵サーバ21-1とIP通信を確立する。ステップS2701において、鍵サーバ21-1のIP通信プログラム155は、代理サーバ503とIP通信を確立する。

【0171】ステップS2510において、代理サーバ503のライセンス管理プログラム761のサーバ認証プログラム781は、鍵サーバ21-1を認証する。ステップS2702において、鍵サーバ21-1の認証プログラム151は、代理サーバ503を認証する。

【0172】例えば、鍵サーバ21-1には、マスター鍵KMSSが予め記憶されており、代理サーバ503に

は、個別鍵KPCCと代理サーバ503のIDが予め記憶されている。代理サーバ503には、更に、マスター鍵KMCCが予め記憶されており、鍵サーバ21-1にも鍵サーバ21-1のIDと個別鍵KPSSが記憶されている。

【0173】鍵サーバ21-1は、代理サーバ503から、代理サーバ503のIDの供給を受け、そのIDと自分自身が有するマスター鍵KMSSにハッシュ関数を適用して、代理サーバ503の個別鍵KPCCと同一の鍵を生成する。

【0174】代理サーバ503は、鍵サーバ21-1から、鍵サーバ21-1のIDの供給を受け、そのIDと自分自身が有するマスター鍵KMCCにハッシュ関数を適用して、鍵サーバ21-1の個別鍵KPSSと同一の鍵を生成する。このようにすることで、代理サーバ503と鍵サーバ21-1の両方に、共通の個別鍵が共有されることになる。これらの個別鍵を用いてさらに、一時的な一時鍵を生成する。

【0175】ステップS2510またはステップS2702における認証の処理に失敗したとき（認証の相手が正当でないと判定されたとき）、処理は終了する。

【0176】ステップS2511において、代理サーバ503の鍵管理プログラム771は、ステップS2503の処理で取得したコンテンツIDを鍵サーバ21-1に送信する。ステップS2703において、鍵サーバ21-1は、代理サーバ503が送信したコンテンツIDを受信する。ステップS2704において、鍵サーバ21-1の鍵配信プログラム152は、鍵保存プログラム153がコンテンツIDと対応づけて保存しているコンテンツ鍵を読み出し、通信ネットワーク4を介して、そのコンテンツ鍵（鍵サーバ21-1と代理サーバ503とで共有する一時鍵で暗号化されている）を代理サーバ503に送信する。ステップS2512において、代理サーバ503の鍵管理プログラム771の鍵受信プログラム783は、鍵サーバ21-1が送信したコンテンツ鍵を受信する。

【0177】ステップS2513において、代理サーバ503の鍵管理プログラム771の鍵配信プログラム784は、ステップS2512の処理で受信したコンテンツ鍵を、鍵サーバ21-1と代理サーバ503とで共有する一時鍵で復号し、電話機一体型端末機501と代理サーバ503で共有する一時鍵で暗号化して、通信ネットワーク4を介して、暗号化されているコンテンツ鍵を電話機一体型端末機501に送信する。ステップS2112において、電話機一体型端末機501の鍵管理プログラム724の受信プログラム731は、代理サーバ503が送信したコンテンツ鍵を受信する。鍵管理プログラム724は、コンテンツ鍵を電話機一体型端末機501と代理サーバ503で共有する一時鍵で復号して、ポータブルメディア3-1の鍵管理プログラム102に供給し、鍵管理プログラム102に、コンテンツ鍵を記憶

させる。

【0178】ステップS2514において、代理サーバ503のコンテンツ管理プログラム772のコンテンツ配信プログラム786は、通信ネットワーク4を介して、暗号化されているコンテンツを電話機一体型端末機501に送信する。ステップS2113において、電話機一体型端末機501のコンテンツ管理プログラム725の受信プログラム732は、代理サーバ503が送信したコンテンツを受信する。

【0179】ステップS2114において、電話機一体型端末機501のPHS/IMT通信プログラム703は、公衆回線網31との接続を切断する。ステップS2202において、公衆回線網31の図示せぬ地上局などは、電話機一体型端末機501と接続を切断する。

【0180】ステップS2115において、電話機一体型端末機501のフォーマット管理プログラム713は、ステップS2113の処理で受信したコンテンツのフォーマットを変換する。コンテンツ管理プログラム725は、フォーマットを変換したコンテンツを、インターフェース609を介して、ポータブルメディア3-1に供給して、コンテンツ管理プログラム103に、コンテンツを記憶させ、処理は終了する。

【0181】次に、電話機一体型端末機501がサーバ5-2からコンテンツをダウンロードする処理を図13および図14のフローチャートを参照して説明する。ステップS3101乃至ステップS3504の処理は、サーバ5-2、並びにIP通信プログラム701、ISP接続プログラム702、PHS/IMT通信プログラム703、およびダウンロードプログラム712により実行され、それぞれ、ステップS2101乃至ステップS2504の処理と同様なので、その説明は省略する。

【0182】ステップS3505において、代理サーバ503のシステム識別プログラム773は、ステップS3503の処理で受信したコンテンツIDを基に、コンテンツおよびコンテンツ鍵のダウンロード先が、サーバ5-2であることを識別する。

【0183】ステップS3506において、代理サーバ503のIP通信プログラム751は、ステップS3505の識別の処理の結果を基に、鍵サーバ21-2とIP通信を確立する。ステップS3701において、鍵サーバ21-2は、代理サーバ503とIP通信を確立する。

【0184】ステップS3507において、代理サーバ503のサーバ認証プログラム781は、鍵サーバ21-2を認証する。ステップS3702において、鍵サーバ21-2は、代理サーバ503を認証する。

【0185】ステップS3507およびステップS3702の処理は、ステップS2510およびステップS2702の処理と同様の処理である。

【0186】ステップS3507またはステップS37

02における認証の処理に失敗したとき（認証の相手が正当でないと判定されたとき）、処理は終了する。

【0187】ステップS3508において、代理サーバ503の鍵管理プログラム771は、ステップS3503の処理で取得したコンテンツIDを鍵サーバ21-2に送信する。ステップS3703において、鍵サーバ21-2は、代理サーバ503が送信したコンテンツIDを受信する。ステップS3704において、鍵サーバ21-2は、コンテンツIDと対応づけて保存しているコンテンツ鍵を読み出し、通信ネットワーク4を介して、そのコンテンツ鍵（鍵サーバ21-2と代理サーバ503とで共有する一時鍵で暗号化されている）を代理サーバ503に送信する。ステップS3509において、代理サーバ503の鍵管理プログラム771の鍵受信プログラム783は、鍵サーバ21-2が送信したコンテンツ鍵を受信する。

【0188】ステップS3510において、代理サーバ503のIP通信プログラム751は、ステップS3505の識別の処理の結果を基に、コンテンツサーバ22-2とIP通信を確立する。ステップS3601において、コンテンツサーバ22-2は、代理サーバ503とIP通信を確立する。

【0189】ステップS3511において、代理サーバ503のコンテンツ管理プログラム772は、ステップS3503の処理で取得したコンテンツIDを、通信ネットワーク4を介して、コンテンツサーバ22-2に送信する。ステップS3602において、コンテンツサーバ22-2は、代理サーバ503が送信したコンテンツIDを受信する。ステップS3603において、コンテンツサーバ22-2は、ステップS3602で受信したコンテンツIDに対応するコンテンツ（暗号化されている）を読み出して、通信ネットワーク4を介して、代理サーバ503に配信する。

【0190】ステップS3512において、代理サーバ503のコンテンツ管理プログラム772の受信プログラム785は、コンテンツサーバ22-2が送信したコンテンツを受信する。

【0191】ステップS3512乃至ステップS3115の処理は、ステップS2513乃至ステップS2115の処理と同様なので、その説明は省略する。

【0192】以上のように、電話機一体型端末機501は、代理サーバ503を介することにより、サーバ5-1からコンテンツおよびコンテンツ鍵をダウンロードするときも、サーバ5-2からコンテンツおよびコンテンツ鍵をダウンロードするときも、いずれの場合も、同一の手順（例えば、コンテンツ鍵を受信してから、コンテンツを受信する）で、コンテンツおよびコンテンツ鍵を受信することができる。

【0193】また、図11乃至図14のフローチャートを参照して説明した手順は、後述する代理サーバ503

がコンテンツの符号化方式および暗号化方式を変換する処理（図16および図17のフローチャートを参照して説明する）に比較して、電話機一体型端末機501が公衆回線網31に接続している時間を短くすることができる。

【0194】次に、図15を参照して、本願のデジタルデータ伝送システムの他の機能の構成について説明する。図10で説明した構成の場合と同一の部分には、図10の場合と同一の番号を付してあり、その説明は省略する。

【0195】図15に示す電話機一体型端末機501は、フォーマット管理プログラム713を有しない。

【0196】図15に示す代理サーバ503のサーバ用LCM514は、ライセンス管理プログラム761およびシーケンス管理プログラム762に加えて、フォーマット管理プログラム801を含む。

【0197】フォーマット管理プログラム801は、コンテンツサーバ22-1または22-2からダウンロードしたコンテンツの符号化方式および暗号化方式をそれぞれ所定の方式に変換する。フォーマット管理プログラム801は、システム識別プログラム811およびフォーマット変換プログラム812から構成されている。

【0198】システム識別プログラム811は、コンテンツのダウンロード先が、サーバ5-1であるか、サーバ5-2であるかのいずれかを識別するためのプログラムである。フォーマット変換プログラム812は、コンテンツの符号化方式および暗号化方式を変換する。

【0199】次に、図15にその構成を示す電話機一体型端末機501および代理サーバ503がサーバ5-2からコンテンツをダウンロードする処理を図16および図17のフローチャートを参照して説明する。

【0200】ステップS4101乃至ステップS4512の処理は、それぞれ、ステップS3101乃至ステップS3512の処理と同様なので、その説明は省略する。

【0201】ステップS4512において、代理サーバ503のフォーマット管理プログラム801は、ステップS4512の処理で受信したコンテンツのフォーマットを変換する。

【0202】ステップS4514において、代理サーバ503の鍵管理プログラム771の鍵配信プログラム784は、ステップS4509の処理で受信したコンテンツ鍵を、鍵サーバ21-2と代理サーバ503とで共有する一時鍵で復号し、電話機一体型端末機501と代理サーバ503で共有する一時鍵で暗号化して、通信ネットワーク4を介して、暗号化されているコンテンツ鍵を電話機一体型端末機501に送信する。ステップS4112において、電話機一体型端末機501の鍵管理プログラム724の受信プログラム731は、代理サーバ503が送信したコンテンツ鍵を受信する。鍵管理プロ

ラム724は、コンテンツ鍵を電話機一体型端末機501と代理サーバ503で共有する一時鍵で復号して、ポータブルメディア3-1の鍵管理プログラム102に供給し、鍵管理プログラム102に、コンテンツ鍵を記憶させる。

【0203】ステップS4515において、代理サーバ503のコンテンツ管理プログラム772のコンテンツ配信プログラム786は、通信ネットワーク4を介して、暗号化されているコンテンツを電話機一体型端末機501に送信する。ステップS4113において、電話機一体型端末機501のコンテンツ管理プログラム725の受信プログラム732は、代理サーバ503が送信したコンテンツを受信する。コンテンツ管理プログラム725は、受信したコンテンツ（フォーマットが変換されている）を、インターフェース609を介して、ポータブルメディア3-1に供給して、コンテンツ管理プログラム103に、コンテンツを記憶させる。

【0204】ステップS4114において、電話機一体型端末機501のPHS/IMT通信プログラム703は、公衆回線網31との接続を切断する。ステップS4202において、公衆回線網31の図示せぬ地上局などは、電話機一体型端末機501と接続を切断して、処理は終了する。

【0205】なお、サーバ5-1からコンテンツおよびコンテンツ鍵を受信する処理は、代理サーバ503がサーバ5-1よりコンテンツを受信した後、サーバ5-1よりコンテンツ鍵を受信する手順となり、同様に行われる。

【0206】このように、代理サーバ503は、サーバ5-1または5-2から受信したコンテンツの符号化方式および暗号化方式を変換して、電話機一体型端末機501に供給することもできる。この場合、電話機一体型端末機501は、コンテンツの符号化方式および暗号化方式を変換するプログラムが不要となる。従って、電話機一体型端末機501は、図10に示す場合に比較して、より少ない演算能力または記憶容量でも、迅速にコンテンツを受信する処理を実行することができる。

【0207】また、コンテンツは、楽音のデータであると説明したが、楽音のデータに限らず、静止画像のデータ、動画のデータ、テキストのデータ、またはプログラムなどでもよい。

【0208】なお、電話機一体型端末機501またはパーソナルコンピュータ502が、コンテンツをダウンロードすると説明したが、電話機一体型端末機501またはパーソナルコンピュータ502に限らず、携帯電話機、PDA（Personal Digital Assistant）、通信機能付き撮像機能付きデジタルビデオカセットレコーダ、通信機能付き電子手帳装置、または携帯型パーソナルコンピュータなどがコンテンツをダウンロードするようにしてもよい。

【0209】また、電話機一体型端末機501は、PHSまたはIMTにより通信すると説明したが、PHSまたはIMTに限らず、W-CDMA (Code Division Multiple Access)、衛星通信、衛星放送、PSTN (Public Switched telephone network)、xDSL (x Digital Subscriber Line)、ISDN (Integrated Services Digital Network)、またはプライベートネットワークなどで通信するようにしてもよい。

【0210】上述した一連の処理は、ハードウェアにより実行させることもできるが、ソフトウェアにより実行させることもできる。一連の処理をソフトウェアにより実行させる場合には、そのソフトウェアを構成するプログラムが、専用のハードウェアに組み込まれているコンピュータ、または、各種のプログラムをインストールすることで、各種の機能を実行することが可能な、例えば汎用のパーソナルコンピュータなどに、プログラム格納媒体からインストールされる。

【0211】コンピュータにインストールされ、コンピュータによって実行可能な状態とされるプログラムを格納するプログラム格納媒体は、図8または図9に示すように、磁気ディスク641若しくは磁気ディスク681 (いずれもフロッピディスクを含む)、光ディスク642若しくは光ディスク682 (いずれも、CD-ROM (Compact Disc-Read Only Memory)、DVD (Digital Versatile Disc)を含む)、光磁気ディスク643若しくは光磁気ディスク683 (いずれもMD (Mini-Disc)を含む)、若しくは半導体メモリ644若しくは半導体メモリ684などよりなるパッケージメディア、または、プログラムが一時的若しくは永続的に格納されるROM602若しくはROM652や、HDD661などにより構成される。プログラム格納媒体へのプログラムの格納は、必要に応じて通信部608または通信部663を介して、ローカルエリアネットワーク、インターネット、デジタル衛星放送といった、有線または無線の通信媒体を利用して行われる。

【0212】なお、本明細書において、プログラム格納媒体に格納されるプログラムを記述するステップは、記載された順序に沿って時系列的に行われる処理はもちろん、必ずしも時系列的に処理されなくとも、並列的あるいは個別に実行される処理をも含むものである。

【0213】また、本明細書において、システムとは、複数の装置により構成される装置全体を表すものである。

【0214】

【発明の効果】請求項1に記載の情報提供装置、請求項3に記載の情報提供方法、および請求項4に記載のプログラム格納媒体によれば、第1の情報処理装置が認証され、第2の情報処理装置または第3の情報処理装置が認証され、第1の情報処理装置からの、コンテンツおよび鍵の送信要求、並びに第2の情報処理装置を特定するデ

ータまたは第3の情報処理装置を特定するデータの受信が制御され、第2の情報処理装置を特定するデータを受信した場合、第2の情報処理装置に対応した手順で、第2の情報処理装置にコンテンツおよび鍵の送信要求を送信するとともに、第2の情報処理装置からコンテンツおよび鍵を受信し、第3の情報処理装置を特定するデータを受信した場合、第3の情報処理装置に対応した手順で、第3の情報処理装置にコンテンツおよび鍵の送信要求を送信するとともに、第3の情報処理装置からコンテンツおよび鍵を受信するように通信が制御され、第1の情報処理装置へのコンテンツおよび鍵の送信が制御されるようにしたので、第1の情報処理装置の処理能力が小さくとも、異なる手順で供給されるコンテンツおよび鍵を受信することができるようになる。

【0215】請求項5に記載の情報処理装置、請求項6に記載の情報処理方法、および請求項7に記載のプログラム格納媒体によれば、第1の情報提供装置が認証され、第1の情報提供装置への、コンテンツおよび鍵の送信要求、並びにコンテンツおよび鍵を提供する第2の情報提供装置を特定するデータ、およびコンテンツおよび鍵を提供する第3の情報提供装置を特定するデータのいずれかの送信が制御され、第2の情報提供装置または第3の情報提供装置から第1の情報提供装置が提供を受け、送信したコンテンツおよび鍵の受信が制御されるようにしたので、処理能力が小さくとも、異なる手順で供給されるコンテンツおよび鍵を受信することができるようになる。

【図面の簡単な説明】

【図1】従来のデジタルデータ伝送システムの構成を示す図である。

【図2】従来のデジタルデータ伝送システムの機能の構成を示す図である。

【図3】パーソナルコンピュータ1がサーバ5-1からコンテンツをダウンロードして、ポータブルデバイス2にチェックアウトする従来の処理を説明するフローチャートである。

【図4】パーソナルコンピュータ1がサーバ5-1からコンテンツをダウンロードして、ポータブルデバイス2にチェックアウトする従来の処理を説明するフローチャートである。

【図5】パーソナルコンピュータ1がサーバ5-2からコンテンツをダウンロードして、ポータブルデバイス2にチェックアウトする従来の処理を説明するフローチャートである。

【図6】パーソナルコンピュータ1がサーバ5-2からコンテンツをダウンロードして、ポータブルデバイス2にチェックアウトする従来の処理を説明するフローチャートである。

【図7】本発明に係るデジタルデータ伝送システムの一実施の形態を示す図である。

【図8】電話機一体型端末機501の構成を説明する図である。

【図9】代理サーバ503の構成を説明する図である。

【図10】本願のデジタルデータ伝送システムの機能の構成を説明する図である。

【図11】電話機一体型端末機501がサーバ5-1からコンテンツをダウンロードする処理を説明するフローチャートである。

【図12】電話機一体型端末機501がサーバ5-1からコンテンツをダウンロードする処理を説明するフローチャートである。

【図13】電話機一体型端末機501がサーバ5-2からコンテンツをダウンロードする処理を説明するフローチャートである。

【図14】電話機一体型端末機501がサーバ5-2からコンテンツをダウンロードする処理を説明するフローチャートである。

【図15】本願のデジタルデータ伝送システムの他の機能の構成を説明する図である。

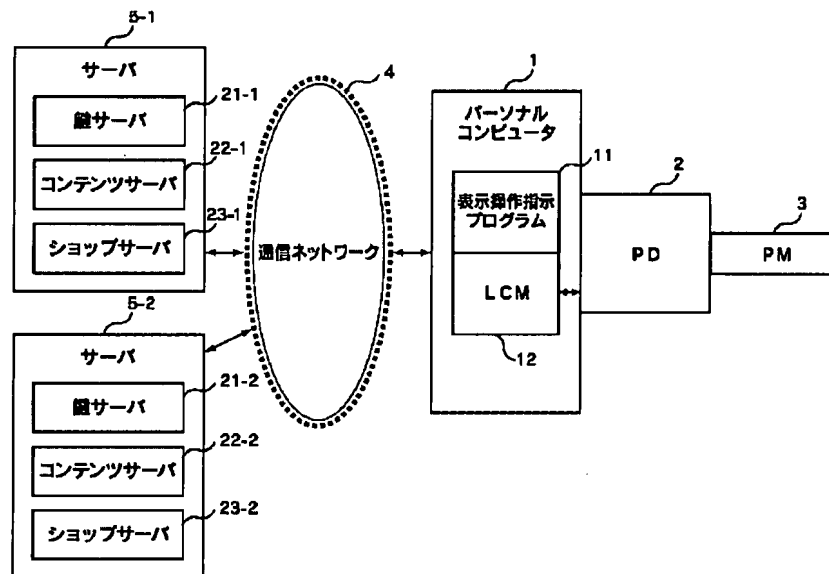
【図16】電話機一体型端末機501がサーバ5-2からコンテンツをダウンロードする処理を説明するフローチャートである。

【図17】電話機一体型端末機501がサーバ5-2からコンテンツをダウンロードする処理を説明するフローチャートである。

【符号の説明】

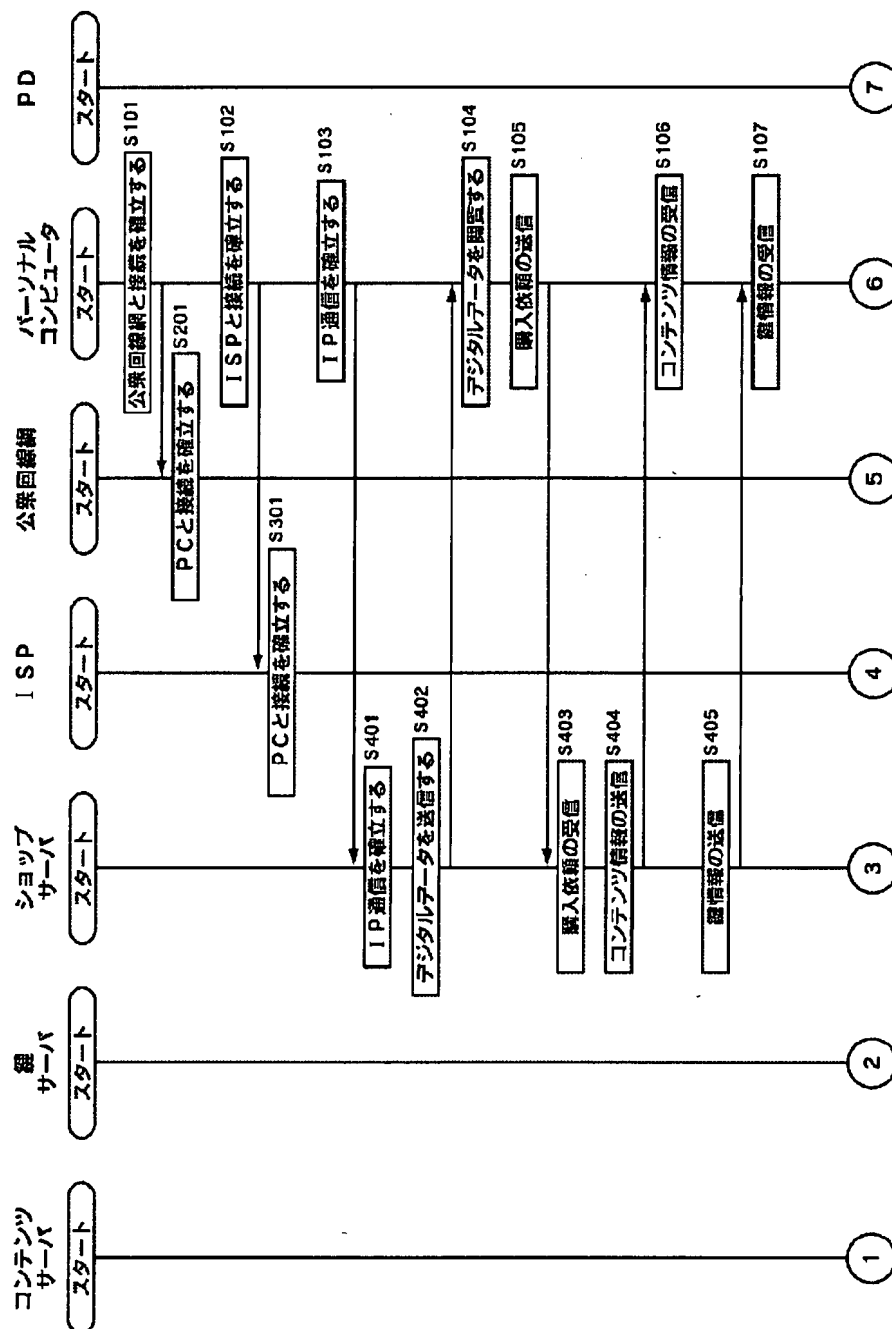
501 電話機一体型端末機, 503 代理サーバ,
511 表示操作指示プログラム, 512 クライアント用LCM, 514 サーバ用LCM, 601 CPU, 602 ROM, 603 RAM, 608 通信部, 641 磁気ディスク, 642 光ディスク, 643 光磁気ディスク, 644 半導体メモリ, 651 CPU, 652 ROM, 653 RAM, 663 通信部, 681 磁気ディスク, 682 光ディスク, 683 光磁気ディスク, 684 半導体メモリ

【図1】



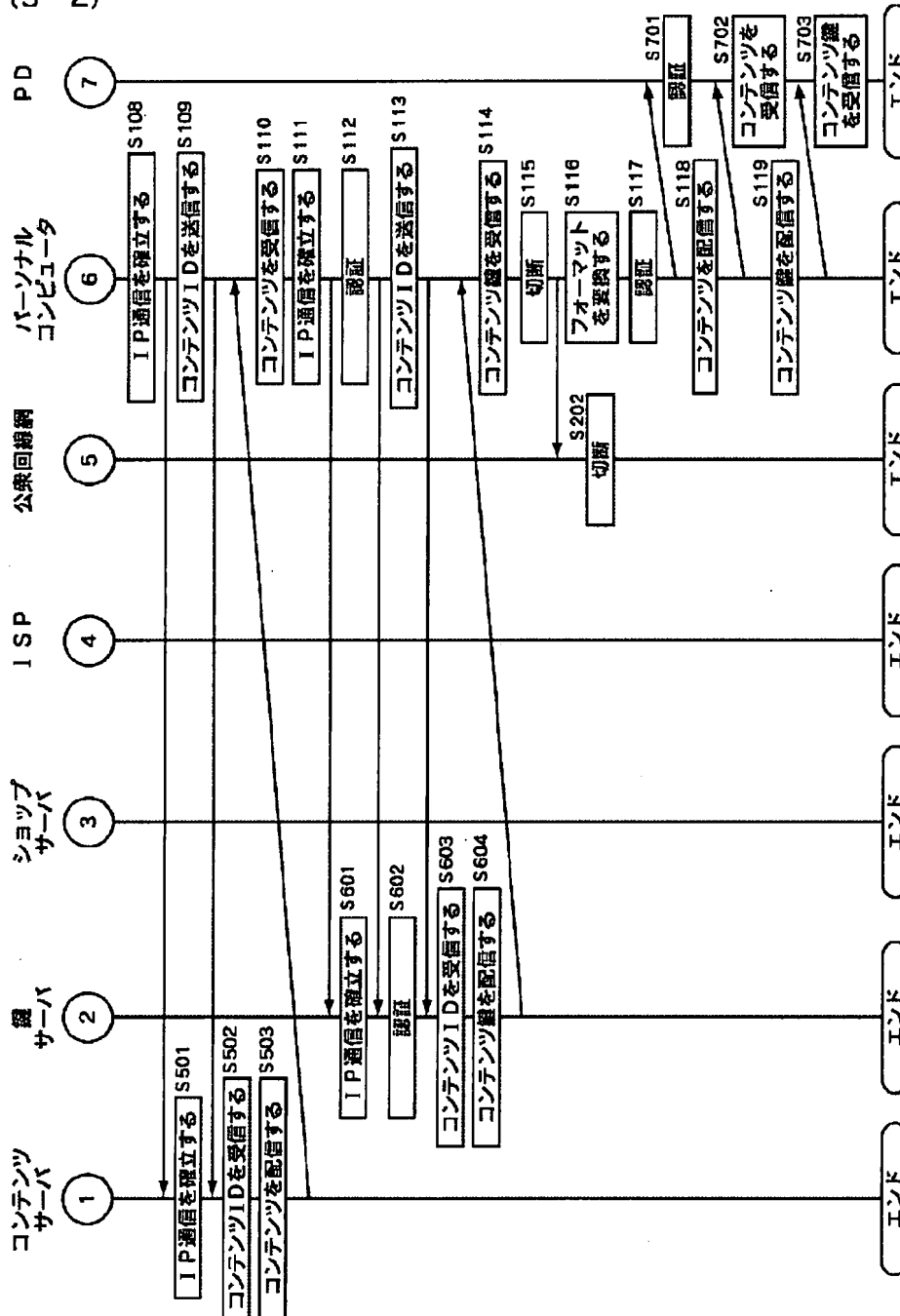
[illegible]

(3-1)



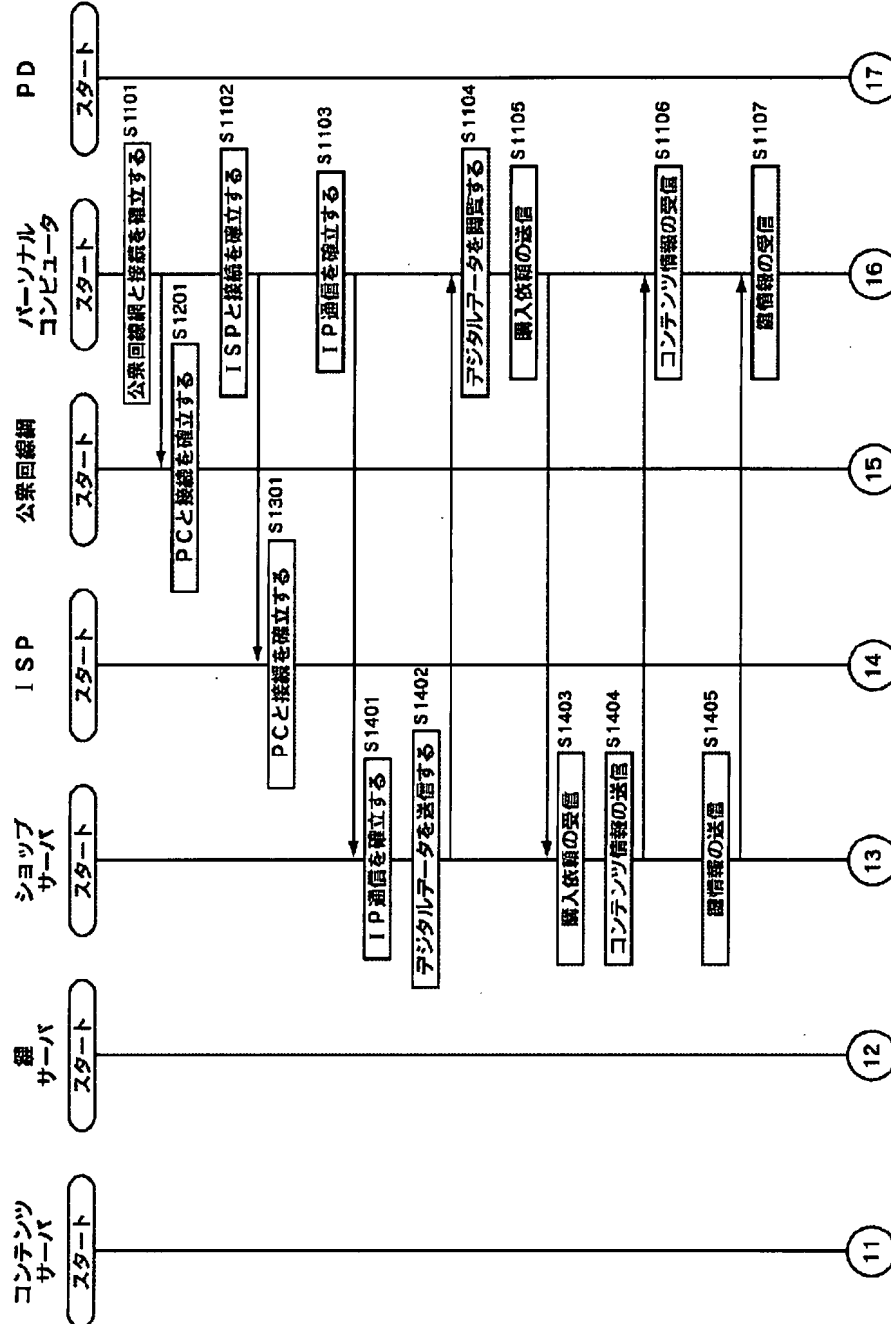
【図4】

(3-2)



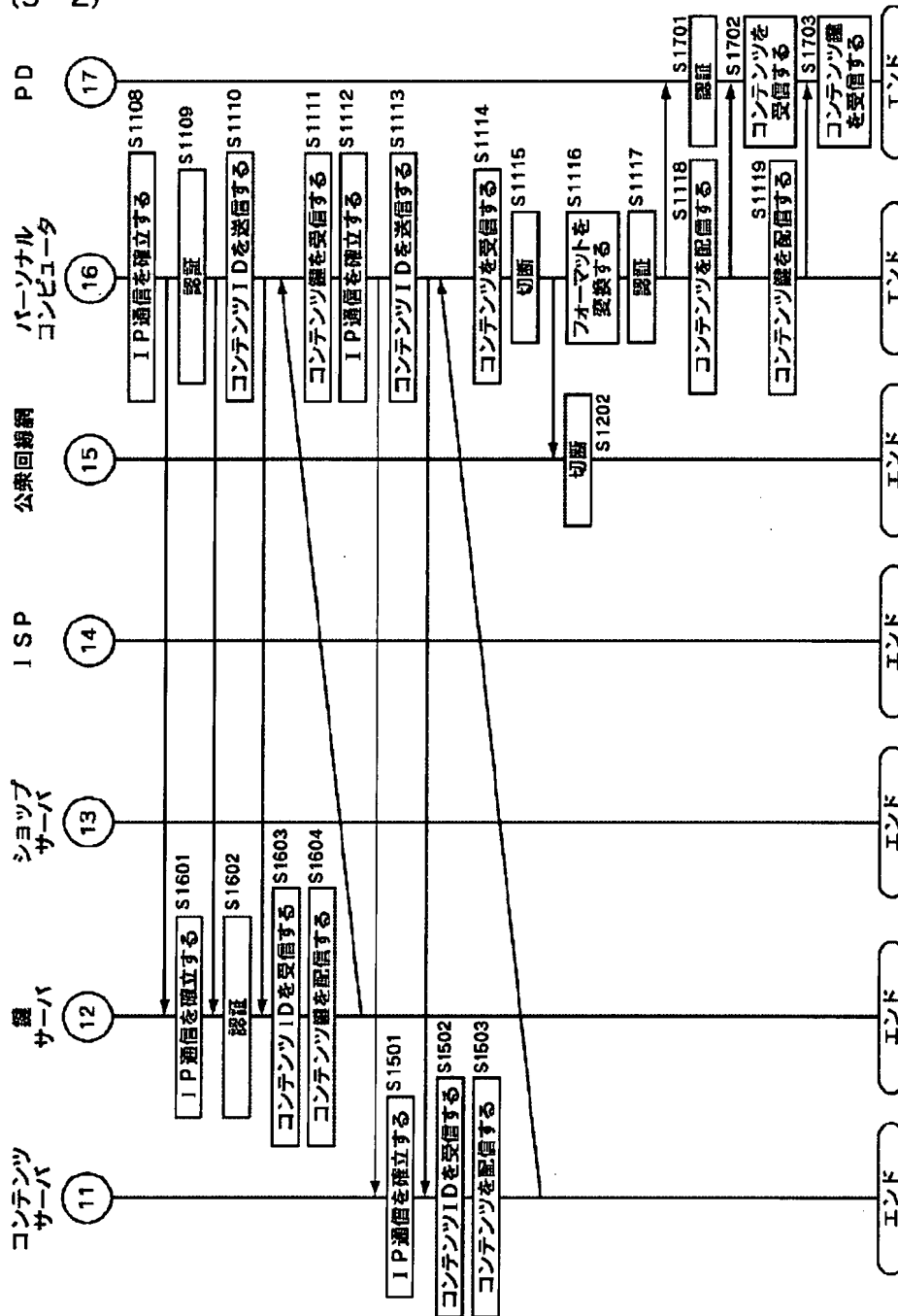
【図5】

(5-1)

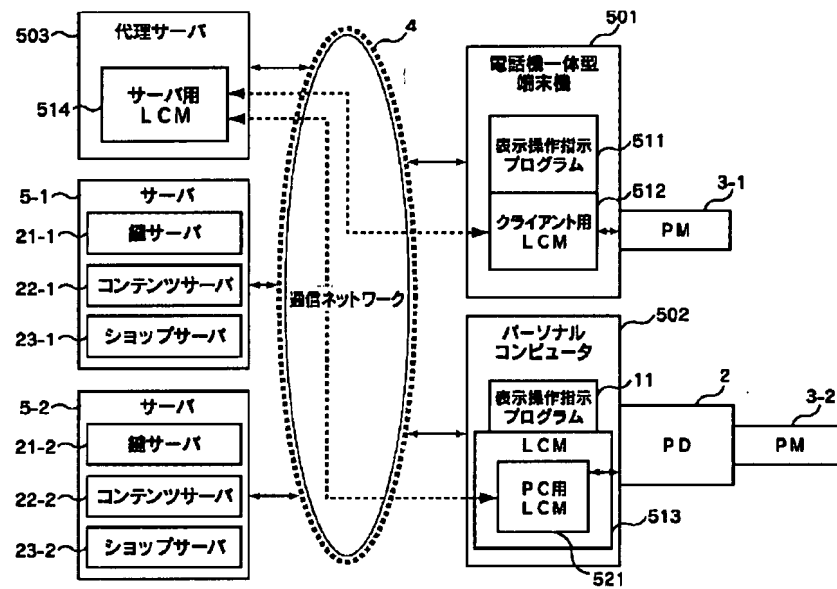


【図6】

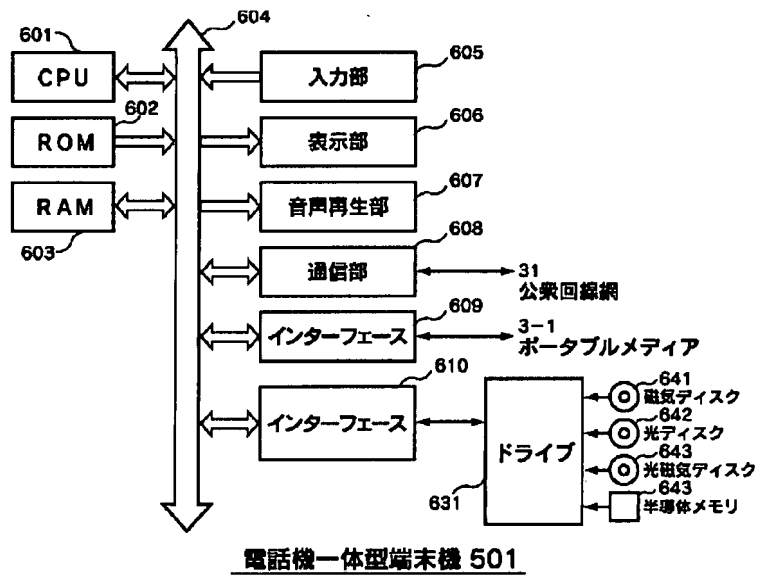
(5-2)



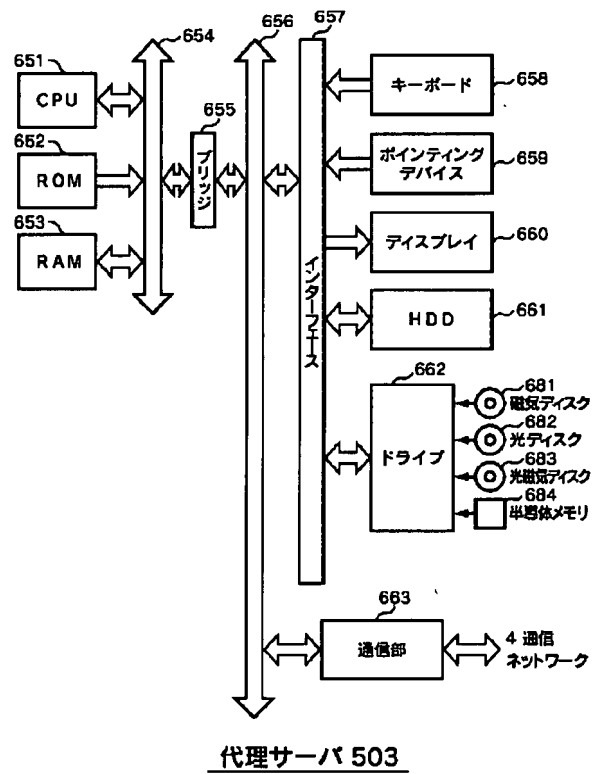
【図7】



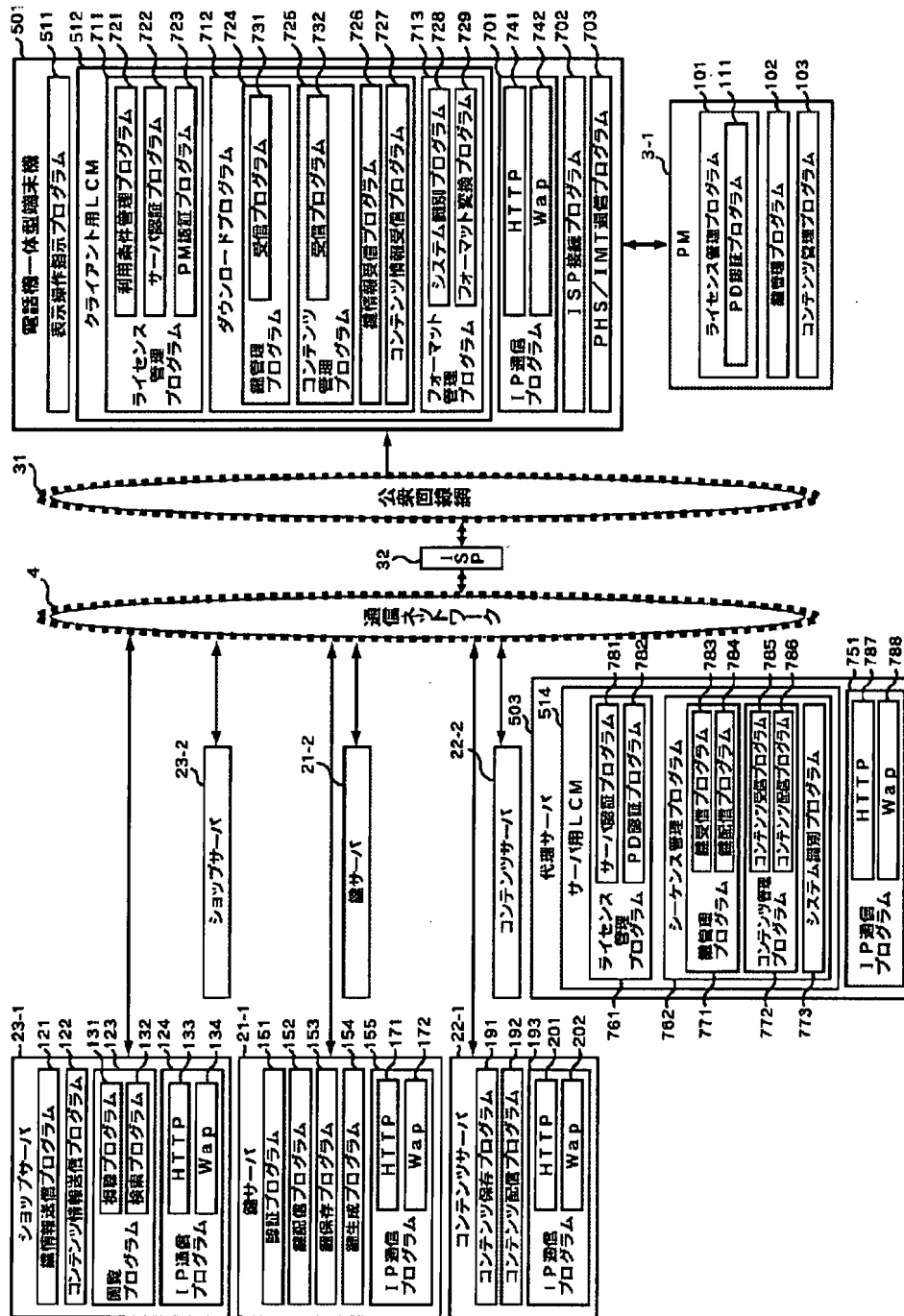
【図8】



【図9】

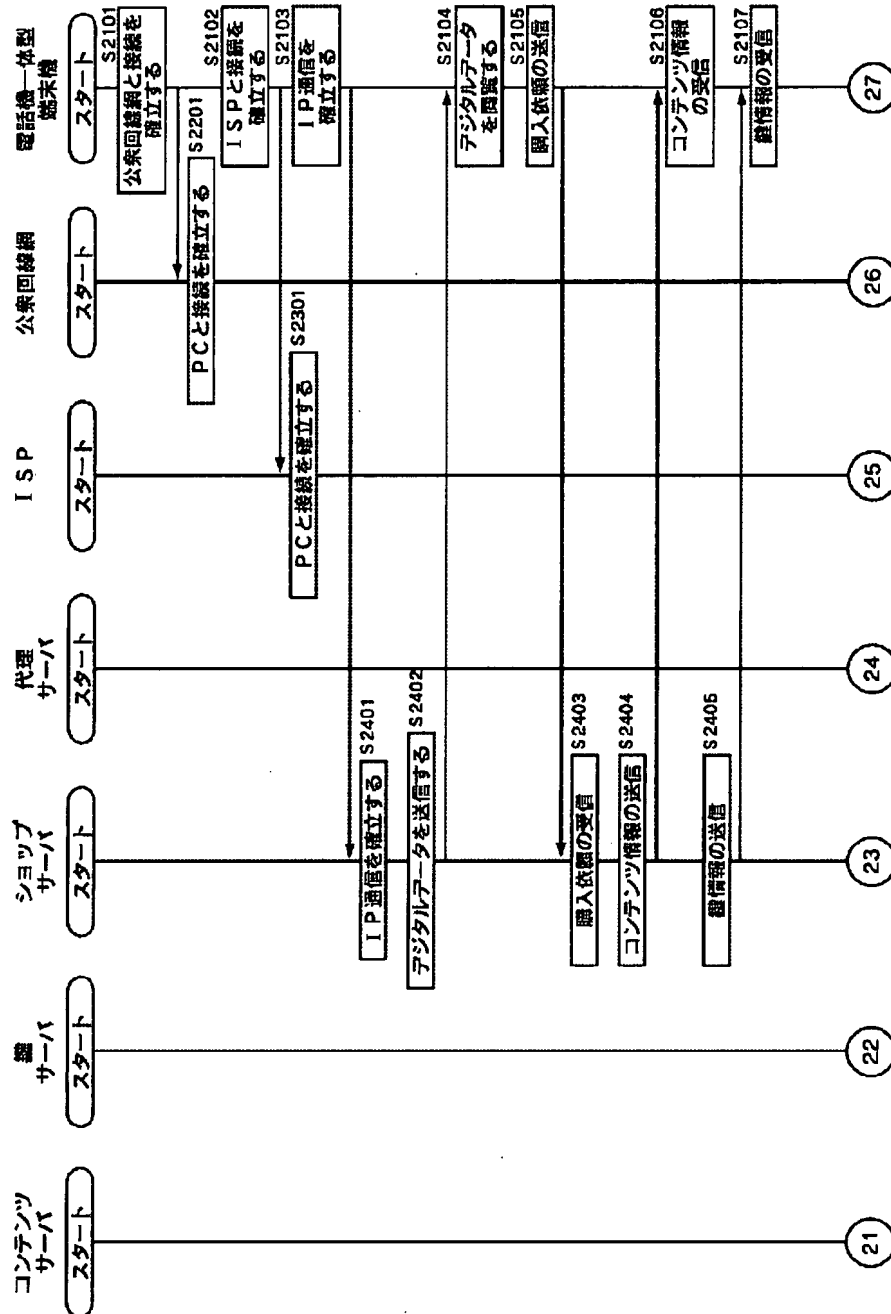


【図10】

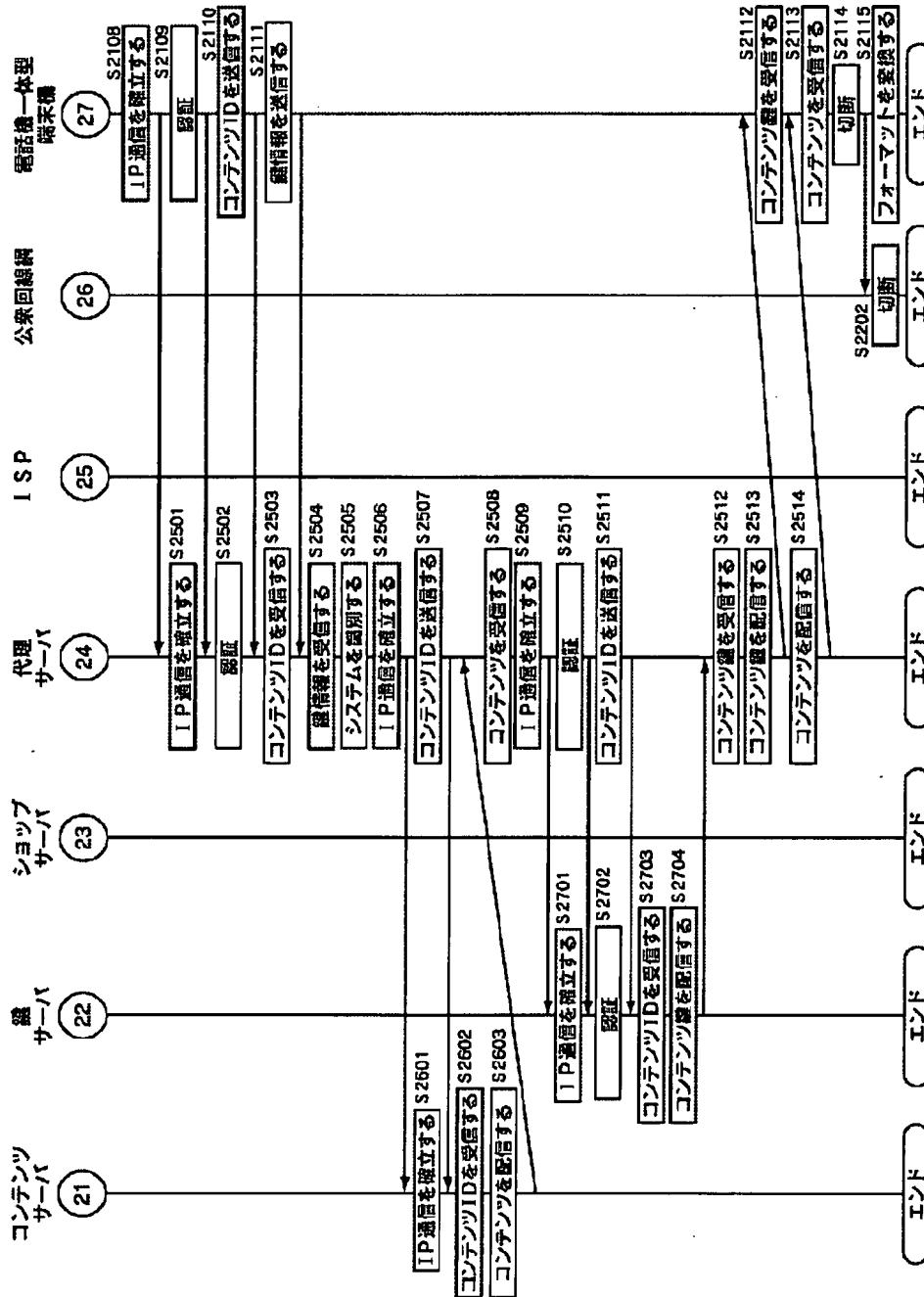


【図11】

(11-1)

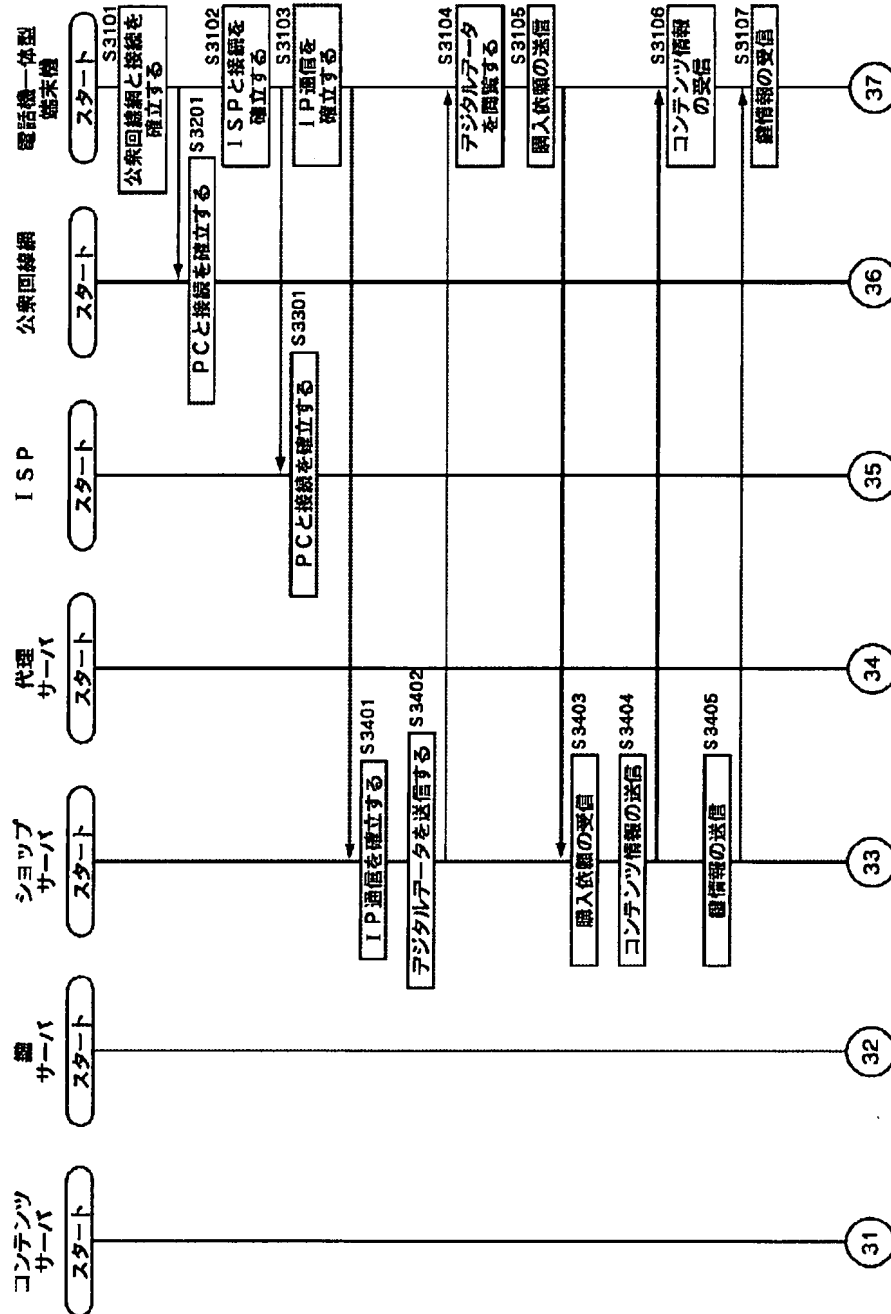


(11-2)

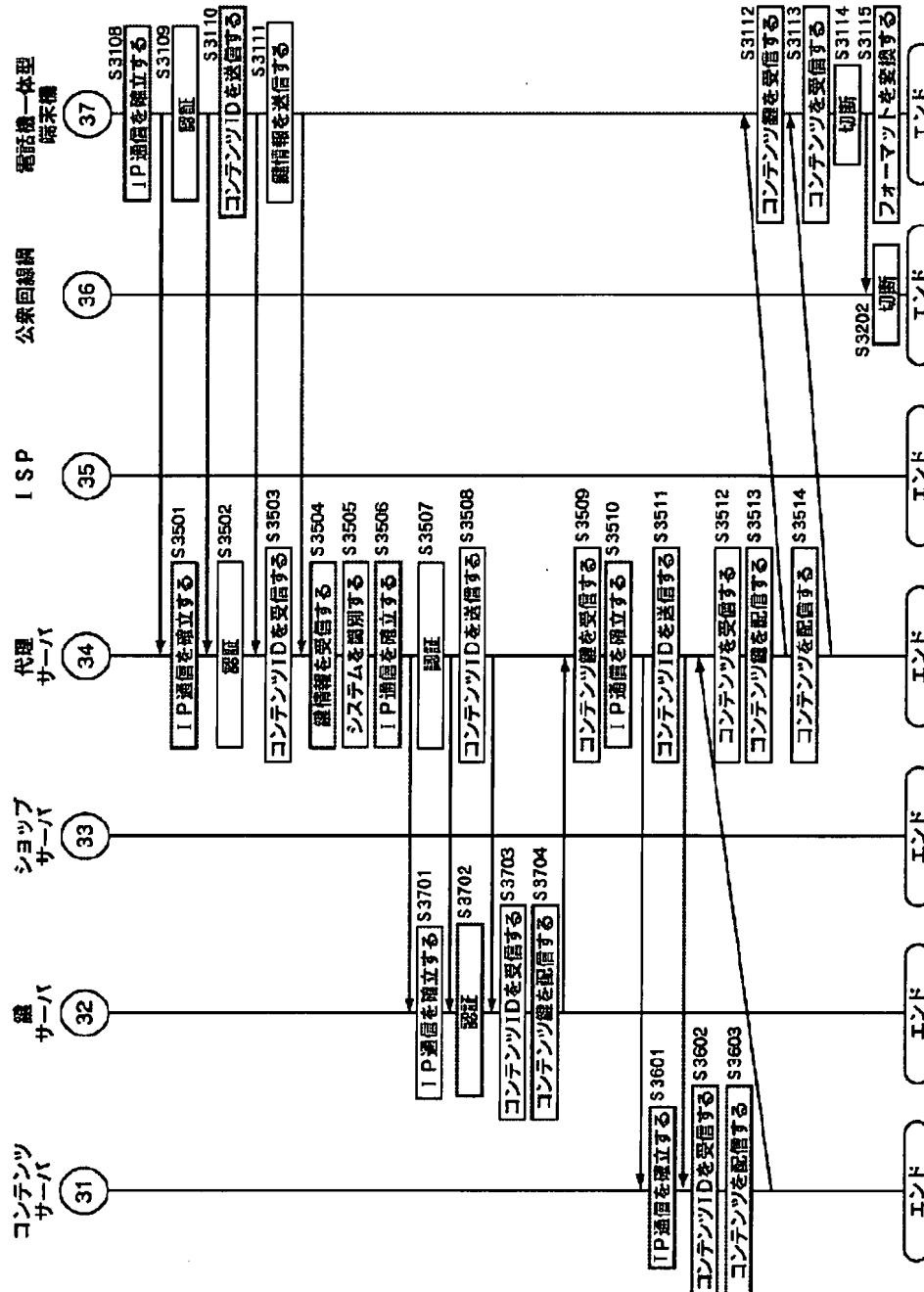


【図13】

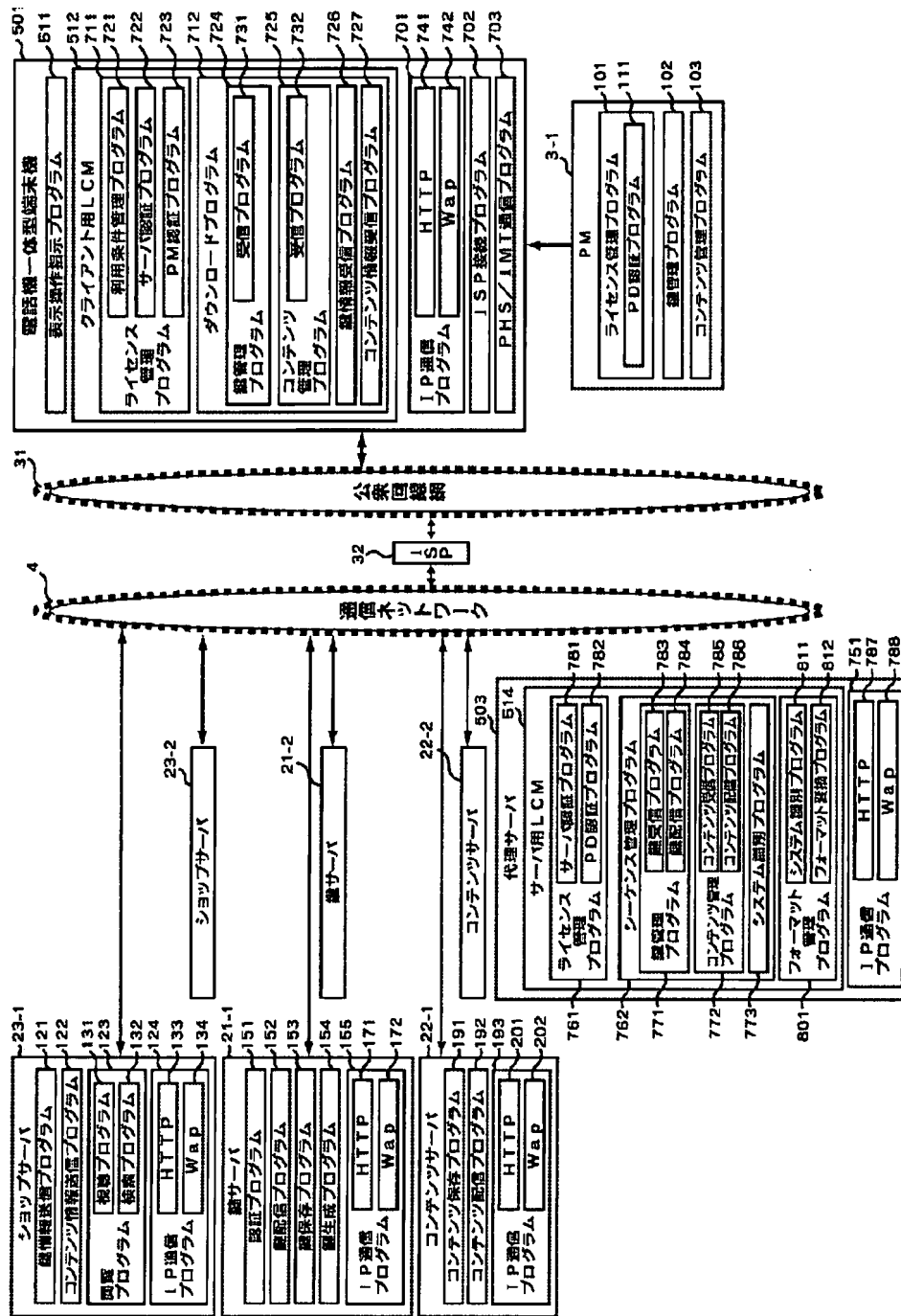
(13-1)



(13-2)

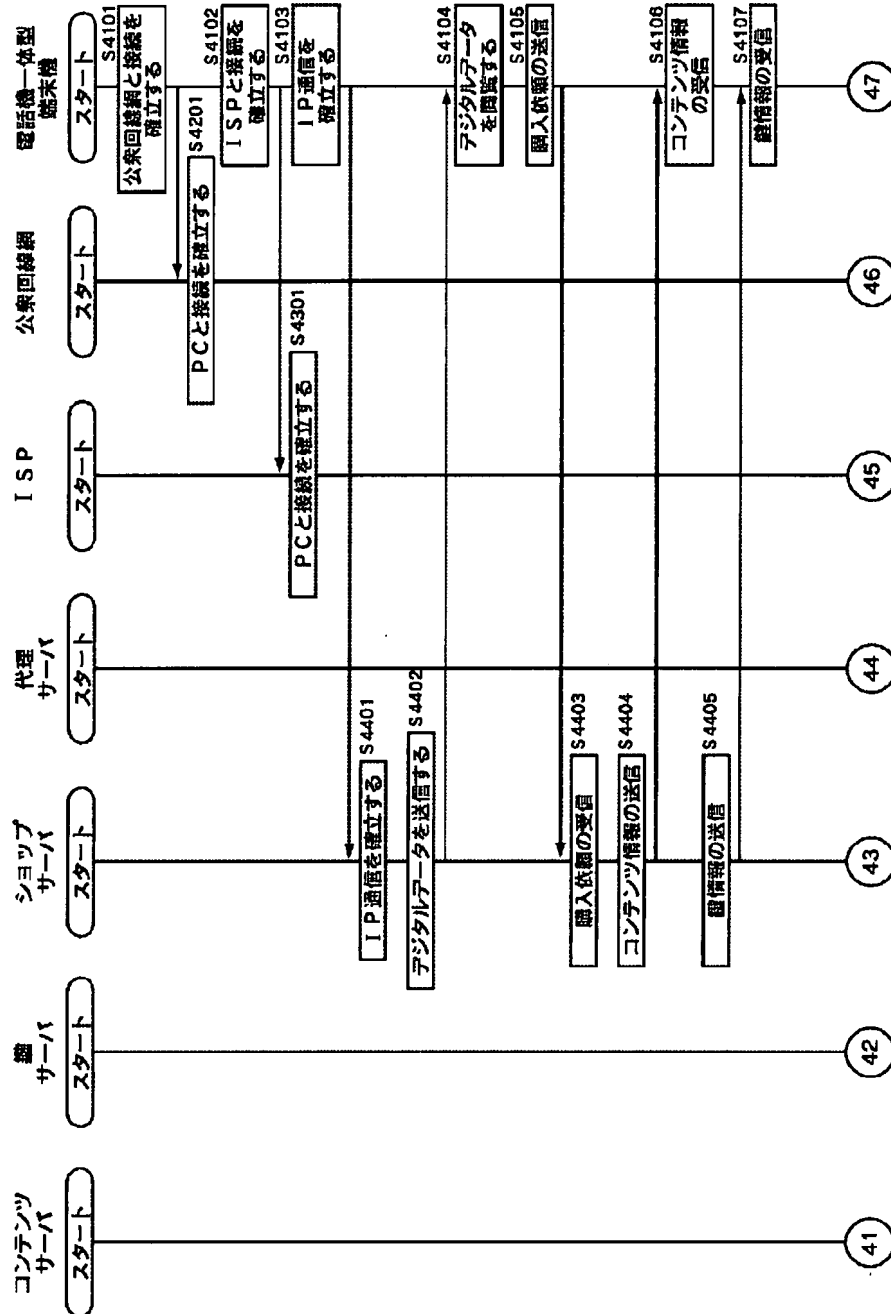


【図15】



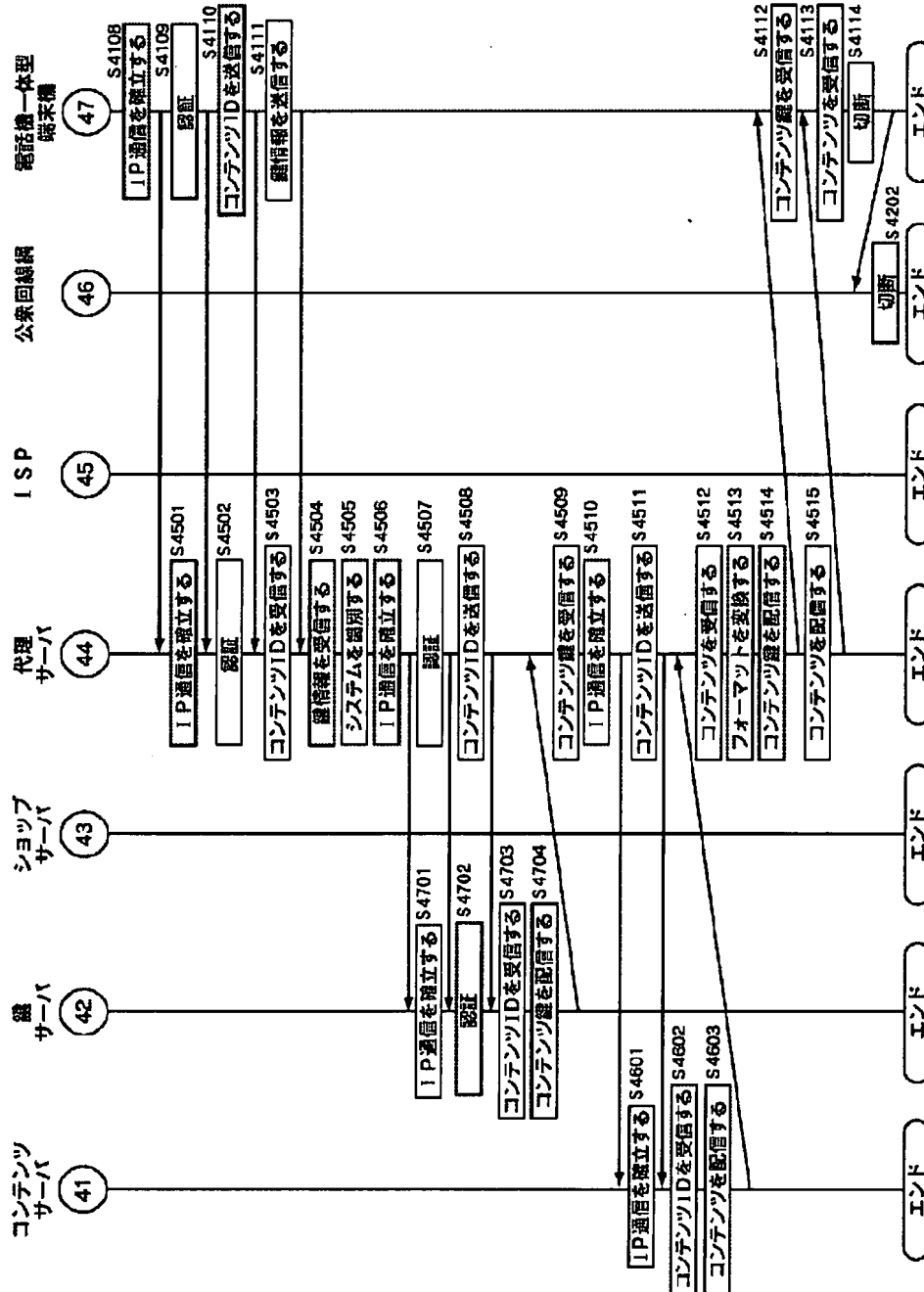
【図16】

(16-1)



【図17】

(16-2)



PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-265361

(43)Date of publication of application : 28.09.2001

(51)Int.Cl. G10K 15/04

H04L 9/08

(21)Application number : 2000-070461 (71)Applicant : SONY CORP

(22)Date of filing : 14.03.2000 (72)Inventor : GO NAOMI

KURIHARA AKIRA

(54) DEVICE AND METHOD FOR PROVIDING INFORMATION, DEVICE AND METHOD FOR PROVIDING INFORMATION, AND PROGRAM STORAGE MEDIUM

(57)Abstract:

PROBLEM TO BE SOLVED: To receive contents and keys supplied by different procedures.

SOLUTION: A license managing program 761 authenticates a telephone set integrated type terminal machine 501 and also authenticates a 1st or 2nd server. An LCM 514 for the servers controls requests the transmission of the contents and keys and controls the reception of data specifying the 1st server or data specifying the 2nd server, and controls communication so that the contents and keys are received from the 1st server by the procedure corresponding to the 1st server when the data specifying the 1st server are received or from the 2nd server by the procedure corresponding to the 2nd server when the data specifying the 2nd server are received. The LCM 514 for the servers controls the transmission of the contents and keys to the telephone set integrated type terminal machine 501.

LEGAL STATUS [Date of request for examination] 28.02.2007

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

* NOTICES *

JPO and INPIT are not responsible for any damages caused by the use of this translation.

1.This document has been translated by computer. So the translation may not reflect the original precisely.

2.**** shows the word which can not be translated.

3.In the drawings, any words are not translated.

CLAIMS

[Claim(s)]

[Claim 1] The 1st authentication means which attests the 1st information processor, and the 2nd authentication means which attests the 2nd information processor or 3rd information processor, A reception-control means to control the reception of data which specifies the data which specify said 2nd information processor as the Request to Send

of the contents and the key from said 1st information processor, and a list, or said 3rd information processor, When said data which specify said 2nd information processor are received, in the procedure corresponding to said 2nd information processor While transmitting the Request to Send of said contents and said key to said 2nd information processor When said contents and said key are received from said 2nd information processor and said data which specify said 3rd information processor are received, in the procedure corresponding to said 3rd information processor While transmitting the Request to Send of said contents and said key to said 3rd information processor Information offer equipment characterized by including a communications control means to control a communication link to receive said contents and said key from said 3rd information processor, and a transmission-control means to control said contents to said 1st information processor, and transmission of said key.

[Claim 2] Information offer equipment according to claim 1 characterized by including further a conversion means to transform either [at least] the coding method of said contents, or the cipher systems into a predetermined coding method or a predetermined cipher system.

[Claim 3] The 1st authentication step which attests the 1st information processor, and the 2nd authentication step which attests the 2nd information processor or 3rd information processor, The reception-control step which controls the reception of data which specifies the data which specify said 2nd information processor as the Request to Send of the contents and the key from said 1st information processor, and a list, or said 3rd information processor, When said data which specify said 2nd information processor are received, in the procedure corresponding to said 2nd information processor While transmitting the Request to Send of said contents and said key to said 2nd information processor When said contents and said key are received from said 2nd information processor and said data which specify said 3rd information processor are received, in the procedure corresponding to said 3rd information processor While transmitting the Request to Send of said contents and said key to said 3rd information processor The information offer approach characterized by including the communications control step which controls a communication link to receive said contents and said key from said 3rd information processor, and the transmission-control step which controls said contents to said 1st information processor, and transmission of said key.

[Claim 4] The 1st authentication step which attests the 1st information processor, and the 2nd authentication step which attests the 2nd information processor or 3rd information processor, The reception-control step which controls the reception of data which specifies the data which specify said 2nd information processor as the Request to Send of the contents and the key from said 1st information processor, and a list, or said 3rd information processor, When said data which specify said 2nd information processor are received, in the procedure corresponding to said 2nd information processor While transmitting the Request to Send of said contents and said key to said 2nd information processor When said contents and said key are received from said 2nd information processor and said data which specify said 3rd information processor are received, in the procedure corresponding to said 3rd information processor While transmitting the Request to Send of said contents and said key to said 3rd information processor The communications control step which controls a communication link to

receive said contents and said key from said 3rd information processor, The program storing medium by which the program which the computer characterized by including the transmission-control step which controls said contents to said 1st information processor and transmission of said key can read is stored.

[Claim 5] An authentication means to attest the 1st information offer equipment, and said 1st information offer equipment, Contents and the Request to Send of a key, the data that specify the 2nd information offer equipment which provides a list with said contents and said key, And a transmission-control means to control transmission of either of the data which specifies the 3rd information offer equipment which offers said contents and said key, The information processor characterized by including a reception-control means for said 1st information offer equipment to receive offer from said 2nd information offer equipment or said 3rd information offer equipment, and to control reception of said contents which transmitted, and said key.

[Claim 6] The authentication step which attests the 1st information offer equipment, and said 1st information offer equipment, Contents and the Request to Send of a key, the data that specify the 2nd information offer equipment which provides a list with said contents and said key, And the transmission-control step which controls transmission of either of the data which specifies the 3rd information offer equipment which offers said contents and said key, The information processing approach characterized by including the reception-control step which said 1st information offer equipment receives offer from said 2nd information offer equipment or said 3rd information offer equipment, and controls reception of said contents which transmitted, and said key.

[Claim 7] The authentication step which attests the 1st information offer equipment, and said 1st information offer equipment, Contents and the Request to Send of a key, the data that specify the 2nd information offer equipment which provides a list with said contents and said key, And the transmission-control step which controls transmission of either of the data which specifies the 3rd information offer equipment which offers said contents and said key, Said 1st information offer equipment receives offer from said 2nd information offer equipment or said 3rd information offer equipment. The program storing medium by which the program which the computer characterized by including the reception-control step which controls reception of said contents which transmitted, and said key can read is stored.

DETAILED DESCRIPTION

[Detailed Description of the Invention]

[0001]

[Field of the Invention] Especially this invention relates to a program storing medium at the information offer equipment and the approach of using the contents which offer the key which decodes contents and contents about a program storing medium in information offer equipment and an approach, an information processor and an approach, and a list, or are enciphered, an information processor and an approach, and a list.

[0002]

[Description of the Prior Art] Drawing 1 is drawing showing the configuration of the conventional digital data transmission system. The personal computer 1 is connected to the communication network 4 which consists of a Local Area Network or the Internet. With cipher systems, such as DES (Data Encryption Standard), it enciphers and a

personal computer 1 is recorded while it changes into the method (for example, ATRAC3 (trademark)) of predetermined compression the data (contents are called hereafter) of the musical sound which received from the contents server 22-1 or 22-2, or was read in CD (Compact Disc).

[0003] A personal computer 1 records the data of use conditions in which the use conditions of contents are shown corresponding to the contents currently enciphered and recorded.

[0004] The data of use conditions show the number (number of the so-called PD which can be checked out mentioned later) of a portable device (Portable Device (it is also called PD)) which can use the contents corresponding to the data of the use condition for coincidence, for example. Even when only the number shown in the data of use conditions checks out contents, a personal computer 1 can reproduce the contents.

[0005] The display operator guidance program 11 of a personal computer 1 inputs directions of check-out etc., and makes LCM (Licensed Compliant Module)12 which is a software module based on the specification of SDMI (Secure Digital Music Initiative) perform processing of the check-out corresponding to the directions etc. while it displays the data (for example, a music name or use conditions etc.) relevant to the contents which the personal computer 1 is recording.

[0006] LCM12 of a personal computer 1 consists of module groups which control to be able to use contents only on the use conditions which a copyright person specifies to each contents for the purpose of prevention of infringement of the copyright by unjust secondary use of contents. Playback conditions, copy conditions, migration conditions, or are recording conditions of contents etc. are included in use conditions.

[0007] LCM12 attests whether the device connected to the personal computer 1 is just, and performs processing of migration of contents etc. by the safe approach. With processing of migration of contents etc., LCM12 generates a required key, manages a key, enciphers contents or controls the communication link with the device connected.

[0008] Moreover, LCM12 checks the justification of the portable media 3 with which it is equipped, adds the use conditions specified by a server 5 to contents (enciphered), and makes contents record.

[0009] LCM12 of a personal computer 1 updates the data of the use conditions corresponding to the contents which supplied them corresponding to having supplied the portable device 2 with the data (for example, a music name or use conditions etc.) relevant to contents while supplying the contents currently enciphered and recorded to the portable device 2 connected (check-out is called hereafter). The count which can check out the data of the use conditions corresponding to the contents which the personal computer 1 is recording on it more when you check out in a detail is reduced by one. Corresponding contents cannot be checked out when the count which can be checked out is 0.

[0010] The portable device 2 makes the portable media 3 with which it is equipped with the data (for example, a music name or use conditions etc.) relevant to contents memorize the contents (namely, checked-out contents) supplied from the personal computer 1.

[0011] The portable media 3 have storages, such as a flash memory, in the interior, and are constituted by the portable device 2 removable.

[0012] Based on the data of the use conditions relevant to contents, the portable device 2 is reproduced and outputs the contents memorized by the portable media 3 with which it is equipped to the headphone which are not illustrated.

[0013] For example, when it is going to reproduce exceeding the count of playback as a playback limit memorized as data of the use conditions relevant to contents, the portable device 2 suspends playback of corresponding contents.

[0014] A user can remove and walk around with the portable device 2 which memorized contents from a personal computer 1, can reproduce the contents memorized by the portable media 3, and can listen to the music corresponding to contents etc. by headphone etc.

[0015] When the portable device 2 is connected to a personal computer 1 through a USB cable etc., the portable device 2 and a personal computer 1 perform processing of mutual recognition. Processing of this mutual recognition is processing of authentication of a challenge response method. A challenge response method is a method which answers with the value (response) which the portable device 2 generated to a certain value (challenge) which a personal computer 1 generates using the private key currently shared with a personal computer 1.

[0016] A server 5-1 distributes the contents which compression coding is carried out by the predetermined method, accumulate the enciphered contents, and are accumulated corresponding to the demand from a personal computer 1. A server 5-1 has the function of the key server 21-1, the contents server 22-1, and the shop server 23-1.

[0017] The key server 21-1 accumulates the contents key for decoding the contents which the contents server 22-1 supplied to the personal computer 1, and supplies a contents key to a personal computer 1 corresponding to the demand of a personal computer 1. Before supply of a contents key, the key server 21-1 and a personal computer 1 perform processing of mutual recognition, and the key server 21-1 enciphers a contents key with a key temporarily which was shared by processing of the mutual recognition, and transmits them to a personal computer 1. A personal computer 1 is decoded with a key temporarily which is sharing the received contents key.

[0018] The contents server 22-1 supplies contents (enciphered) to a personal computer 1 with the use conditions corresponding to contents through a communication network 4 corresponding to the demand of a personal computer 1.

[0019] While the shop server 23-1 provides a personal computer 1 with the digital data (the list of the contents containing the music name of contents, a price, etc. is included) relevant to the contents which the contents server 22-1 supplies. It corresponds to the application of the purchase of the contents from a personal computer 1. URL (Uniform Resource Locator) of the contents server 22-1 which supplies the contents, URL of the key server 21-1 which supplies the contents key which decodes the contents, etc. are supplied to a personal computer 1.

[0020] A server 5-2 distributes the contents which compression coding is carried out by the predetermined method, accumulate the enciphered contents, and are accumulated corresponding to the demand from a personal computer 1. A server 5-2 has the function of the key server 21-2, the contents server 22-2, and the shop server 23-2.

[0021] The key server 21-2 accumulates the contents key for decoding the contents which the contents server 22-2 supplied to the personal computer 1, and supplies a contents key to a personal computer 1 corresponding to the demand of a personal

computer 1. Before supply of a contents key, the key server 21-2 and a personal computer 1 perform processing of mutual recognition, and the key server 21-2 enciphers a contents key with a key temporarily which was shared by processing of the mutual recognition, and transmits them to a personal computer 1. A personal computer 1 is decoded with a key temporarily which is sharing the received contents key.

[0022] The contents server 22-2 supplies contents (enciphered) to a personal computer 1 with the use conditions corresponding to contents through a communication network 4 corresponding to the demand of a personal computer 1.

[0023] While the shop server 23-2 provides a personal computer 1 with the digital data (the list of the contents containing the music name of contents, a price, etc. is included) relevant to the contents which the contents server 22-2 supplies It corresponds to the application of the purchase of the contents from a personal computer 1. URL of the contents server 22-2 which supplies the contents, URL of the key server 21-2 which supplies the contents key which decodes the contents, etc. are supplied to a personal computer 1.

[0024] Hereafter, when it is not necessary to distinguish a server 5-1 and a server 5-2 separately, a server 5 is only called. Hereafter, when it is not necessary to distinguish the key server 21-1 and the key server 21-2 separately, the key server 21 is only called. Hereafter, when it is not necessary to distinguish the contents server 22-1 and the contents server 22-2 separately, the contents server 22 is only called. Hereafter, when it is not necessary to distinguish the shop server 23-1 and the shop server 23-2 separately, the shop server 23 is only called.

[0025] Next, with reference to drawing 2 , the configuration of the function of the conventional digital data transmission system is explained. In addition to the display operator guidance program 11 and LCM12, a personal computer 1 performs the IP (Internet Protocol) communications program 13, the ISP (Internet Service Provider) connection program 14, and the PHS (Personal Handyphone System) / IMT (International Mobile Telecommunication System) communications program 15.

[0026] The PHS/IMT communications program 15 is a program for communicating through the public line network 31. The ISP connection program 14 is a program for connecting with ISP32. The IP communications program 13 is a program for including procedures, such as HTTP (Hypertext Transport Protocol)⁷⁴ and Wap (Wireless Access Protocol)⁷⁵, and communicating with the key server 21, the contents server 22, or the shop server 23 through a communication network 4.

[0027] LCM12 consists of the license manager 51, a download program 52-1, a download program 52-2, and a format manager 53.

[0028] The license manager 51 is a program for managing the use of contents based on the use conditions of contents, and consists of a use condition manager 61, a CD ripping program 62, and a PD authentication program 63.

[0029] The use condition manager 61 updates the data of use conditions corresponding to check-out of contents etc. while performing management of whether check-out of the contents which the personal computer 1 is recording etc. is permitted based on the use conditions of contents, or to forbid. CD ripping program 62 generates the use conditions corresponding to the read contents while reading contents from CD with which the personal computer 1 was equipped.

[0030] PD authentication program 63 attests the portable device 2 with which the personal computer 1 is equipped.

[0031] The download program 52-1 is a program for downloading contents and a contents key from a server 5-1, and consists of the key manager 64, a contents manager 65, a key information receiving agent 66, and a contents information receiving agent 67.

[0032] The key manager 64 performs processing of authentication of the key server 21-1, receives a contents key from the key server 21-1, is made to run on contents, and manages a contents key. The key manager 64 consists of a server authentication program 71 and a receiving agent 72.

[0033] The server authentication program 71 attests the key server 21-1 by processing mentioned later. A receiving agent 72 receives a contents key from the key server 21-1 through a communication network 4.

[0034] Through a communication network 4, the contents manager 65 receives contents with the data of the use conditions of contents from the contents server 22-1, and records contents with the data of the use conditions of contents. The receiving agent 73 of the contents manager 65 receives the data and contents of use conditions of contents from the contents server 22-1.

[0035] The key information receiving agent 66 receives URL which specifies the key server 21-1 which supplies the contents key corresponding to desired contents from the shop server 23-1. The contents information receiving agent 67 receives URL which specifies the content ID which specifies the contents for which a user asks from the shop server 23-1, and the contents server 22-1 which supplies the contents.

[0036] The download program 52-2 is a program for downloading contents and a contents key from a server 5-2, and since it has the same configuration as the download program 52-1, it omits the explanation.

[0037] The format manager 53 encodes the contents read from CD by the predetermined method, and enciphers while it transforms into a predetermined method the coding method and cipher system of contents which were downloaded from the contents server 22-1 or 22-2, respectively. The format manager 53 consists of a system discernment program 68 and a format conversion program 69.

[0038] The system discernment program 68 is a program for the download place of contents to identify whether it is a server 5-1 or it is a server 5-2. The format conversion program 69 changes the coding method and cipher system of contents.

[0039] The portable device 2 performs the license manager 81, the key manager 82, and the contents manager 83.

[0040] The license manager 81 consists of a use condition manager 91 which manages the count of playback of contents etc. based on the use conditions corresponding to contents, a PC authentication program 92 which attests a personal computer 1, and a PM authentication program 93 which attests the portable media 3.

[0041] Make it encipher with the key for preservation with which the portable media 3 have memorized beforehand the contents key supplied from the personal computer 1, and the portable media 3 are made to memorize the key manager 82, and it is managed.

[0042] The contents manager 83 makes the portable media 3 memorize the contents supplied from the personal computer 1, and manages them.

[0043] The portable media 3 perform the license manager 101, the key manager 102, and the contents manager 103.

[0044] The license manager 101 has PD authentication program 111 which attests the portable device 2, memorizes the data of the use conditions corresponding to contents, and controls read-out of contents etc. based on the data of use conditions. The key manager 102 enciphers, memorizes and manages the contents key supplied from the portable device 2 with the key for preservation memorized beforehand. The contents manager 103 memorizes and manages the contents supplied from the portable device 2.

[0045] The shop server 23-1 performs the key information transmitting program 121, the contents information transmitting program 122, the perusal program 123, and the IP communications program 124.

[0046] The key information transmitting program 121 transmits URL of the key server 21-1 which supplies the contents key corresponding to the contents for which the user of a personal computer 1 asks in a personal computer 1 through a communication network 4.

[0047] The contents information transmitting program 122 transmits URL of the contents server 22-1 which supplies the contents for which the user of a personal computer 1 asks in a personal computer 1 through a communication network 4.

[0048] The perusal program 123 consists of a viewing-and-listening program 131 which makes the user of a personal computer 1 view and listen to contents, and a retrieval program 132 whose user of a personal computer 1 searches desired contents.

[0049] The IP communications program 124 is a program for including procedures, such as HTTP133 and Wap134, and communicating with a personal computer 1 through a communication network 4.

[0050] The key server 21-1 performs the authentication program 151, the key distribution program 152, the key preservation program 153, the key generator 154, and the IP communications program 155.

[0051] The authentication program 151 is a program which attests a personal computer 1 etc. The key distribution program 152 is a program which distributes the contents key which the key preservation program 153 saves in the attested personal computer 1. The key preservation program 153 is a program which saves the contents key generated by the key generator 154. The key generator 154 is a program which is made to run on contents and generates a contents key.

[0052] The IP communications program 155 is a program for including procedures, such as HTTP171 and Wap172, and communicating with a personal computer 1 etc. through a communication network 4.

[0053] The contents server 22-1 performs the contents preservation program 191, the contents distribution program 192, and the IP communications program 193.

[0054] The contents preservation program 191 makes the contents enciphered correspond with content ID, and saves them. The contents distribution program 192 distributes the contents corresponding to content ID which the contents preservation program 191 saves to a personal computer 1, when there is a demand from a personal computer 1.

[0055] The IP communications program 193 is a program for including procedures, such as HTTP201 and Wap202, and communicating with a personal computer 1 through a communication network 4.

[0056] Since it has the same configuration as the shop server 23-1, the shop server 23-2 omits the explanation. Since it has the same configuration as the key server 21-1, the key server 21-2 omits the explanation. Since it has the same configuration as the contents server 22-1, the contents server 22-2 omits the explanation.

[0057] Next, a personal computer 1 downloads contents from a server 5-1, and the conventional processing which he checks out to the portable device 2 is explained with reference to the flow chart of drawing 3 and drawing 4 . In step S101, PHS / IMT communications program 15 of a personal computer 1 establish the public line network 31 and connection. In step S201, the earth station which the public line network 31 does not illustrate establishes a personal computer 1 and connection.

[0058] In step S102, the ISP connection program 14 of a personal computer 1 establishes ISP32 and connection. In step S301, ISP32 establishes a personal computer 1 and connection.

[0059] In step S103, the IP communications program 13 of a personal computer 1 establishes the shop server 23 and IP communication link. In step S401, the IP communications program 124 of the shop server 23-1 establishes a personal computer 1 and IP communication link.

[0060] In step S402, the perusal program 123 of the shop server 23-1 transmits the digital data for perusal (for selection of contents) to a personal computer 1 through a communication network 4. The browser program which a personal computer 1 does not illustrate displays an image or a text corresponding to digital data etc., and a user is made to peruse it in step S104. Moreover, the browser program of a personal computer 1 makes a user try listening contents by streaming playback of contents, or makes the perusal program 123 of the shop server 23-1 search contents by the keyword, and displays the result. Processing of step S402 and step S104 is repeated corresponding to a demand of the user of a personal computer 1.

[0061] In step S105, the browser program of a personal computer 1 transmits a purchase request to the shop server 23-1. In step S403, the perusal program 123 of the shop server 23-1 receives the purchase request transmitted from the personal computer 1.

[0062] In step S404, the contents information transmitting program 122 of the shop server 23-1 transmits the contents information containing the content ID for specifying URL and contents of the contents server 22-1 which distribute the contents corresponding to the purchase request which received by processing of step S403 etc. to a personal computer 1 through a communication network 4. In step S106, the contents information receiving agent 67 of a personal computer 1 receives the contents information which the shop server 23-1 transmitted.

[0063] In step S405, the key information transmitting program 121 of the shop server 23-1 transmits key information, such as URL of the key server 21-1 which distributes the contents key of the contents corresponding to the purchase request which received by processing of step S403, to a personal computer 1 through a communication network 4. In step S107, the key information receiving agent 66 of a personal computer 1 receives the key information which the shop server 23-1 transmitted.

[0064] In step S108, the IP communications program 13 of a personal computer 1 establishes the contents server 22-1 and IP communication link based on URL of the contents server 22-1 contained in the contents information acquired by processing of

step S106. In step S501, the IP communications program 193 of the contents server 22-1 establishes a personal computer 1 and IP communication link.

[0065] In step S109, the contents manager 65 of a personal computer 1 transmits the content ID acquired by processing of step S106 to the contents server 22-1 through a communication network 4. In step S502, the contents server 22-1 receives the content ID which the personal computer 1 transmitted. In step S503, the contents distribution program 192 of the contents server 22-1 reads the contents (enciphered) corresponding to the content ID which received at step S502 from the contents preservation program 191, and distributes them to a personal computer 1 through a communication network 4. In step S110, the receiving agent 73 of the contents manager 65 of a personal computer 1 receives the contents which the contents server 22-1 transmitted.

[0066] In step S111, the IP communications program 13 of a personal computer 1 establishes the key server 21-1 and IP communication link based on URL of the key server 21-1 contained in the key information acquired by processing of step S107. In step S601, the IP communications program 155 of the key server 21-1 establishes a personal computer 1 and IP communication link.

[0067] In step S112, the server authentication program 71 of the key manager 64 of a personal computer 1 attests the key server 21-1. In step S602, the authentication program 151 of the key server 21-1 attests a personal computer 1.

[0068] The master key KMS is beforehand memorized by the key server 21-1, and ID of the individual key KPP and a personal computer 1 is beforehand memorized by the personal computer 1. The master key KMP is further memorized beforehand by the personal computer 1, and ID and the individual key KPS of the key server 21-1 are memorized by the key server 21-1.

[0069] The key server 21-1 receives supply of ID of a personal computer 1 to the personal computer 1, applies a Hash Function to the master key KMS which the ID and themselves have, and generates the same key as the individual key KPP of a personal computer 1.

[0070] A personal computer 1 receives supply of ID of the key server 21-1 to the key server 21-1, applies a Hash Function to the master key KMP which the ID and themselves have, and generates the same key as the individual key KPS of the key server 21-1. A personal computer 1 and an individual key common to both key servers 21-1 will be shared between doing in this way. A key is further generated temporarily using these individual keys.

[0071] In step S113, the key manager 64 of a personal computer 1 transmits content ID to the key server 21-1. In step S603, the key server 21-1 receives the content ID which the personal computer 1 transmitted. In step S604, the key distribution program 152 of the key server 21-1 reads the contents key which the key preservation program 153 matches with content ID, and is saved, and transmits the contents key (enciphered with the key temporarily) to a personal computer 1 through a communication network 4. In step S114, the receiving agent 72 of the key manager 64 of a personal computer 1 receives the contents key which the key server 21-1 transmitted. The key manager 64 decodes the received contents key with a key temporarily.

[0072] In step S115, the PHS/IMT communications program 15 of a personal computer 1 cuts connection with the public line network 31. In step S202, the earth station which the public line network 31 does not illustrate cuts connection with a personal computer 1.

[0073] In step S116, the format manager 53 transforms into a predetermined method the coding method and cipher system of contents which were received by processing of step S110, respectively.

[0074] When the user of a personal computer 1 directs check-out of the contents which received to the display operator guidance program 11, processing after step S117 is performed.

[0075] In step S117, PD authentication program 63 of the license manager 51 of a personal computer 1 attests the portable device 2. In step S701, PC authentication program 92 of the license manager 81 of the portable device 2 attests a personal computer 1.

[0076] Processing of the mutual recognition of the personal computer 1 and the portable device 2 in step S117 and step S701 is processing of authentication of a challenge response method, and there are few amounts of operations as compared with processing of the mutual recognition of the key server 21-1 and personal computer 1 in step S112 and step S602. A personal computer 1 and the portable device 2 are the same operations, and generate and share a key from a response temporarily, respectively.

[0077] In step S118, the contents manager 65 of a personal computer 1 distributes the contents enciphered to the portable device 2. In step S702, the contents manager 83 of the portable device 2 receives the contents which the personal computer 1 distributed, and supplies them to the contents manager 103 of the portable media 3. The contents manager 103 of the portable media 3 memorizes contents.

[0078] In addition, when the portable device 2 is equipped with the portable media 3, mutual recognition of the portable device 2 and the portable media 3 is carried out.

[0079] In step S119, the key manager 64 of a personal computer 1 distributes the contents key (enciphered with the key temporarily which is shared between the portable device 2 and the portable media 3) corresponding to the contents distributed to the portable device 2 at step S118. In step S703, the key manager 82 of the portable device 2 receives the contents key which the personal computer 1 distributed, and supplies it to the key manager 102 of the portable media 3. The key manager 102 of the portable media 3 decodes a contents key with a key temporarily, and memorizes a contents key.

[0080] Next, a personal computer 1 downloads contents from a server 5-2, and the processing which he checks out to the portable device 2 is explained with reference to the flow chart of drawing 5 and drawing 6. Processing of step S1101 thru/or step S1107 is performed by a server 5-2 and the list by the IP communications program 13, the ISP connection program 14, the PHS/IMT communications program 15, and the download program 52-2, and since it is the same as that of processing of step S101 thru/or step S107, the explanation is omitted, respectively.

[0081] In step S1108, the IP communications program 13 of a personal computer 1 establishes the key server 21-2 and IP communication link based on URL of the key server 21-2 contained in the key information acquired by processing of step S1107. In step S1601, the key server 21-2 establishes a personal computer 1 and IP communication link.

[0082] In step S1109, the download program 52-2 of a personal computer 1 attests the key server 21-2. In step S1602, the key server 21-2 attests a personal computer 1.

Processing of step S1109 and step S1602 is the same processing as processing of step S112 and step S602.

[0083] In step S1110, the download program 52-2 of a personal computer 1 transmits content ID to the key server 21-2. In step S1603, the key server 21-2 receives the content ID which the personal computer 1 transmitted. In step S1604, the key server 21-2 reads the contents key which matches with content ID and is saved, and transmits the contents key (enciphered with the key temporarily) to a personal computer 1 through a communication network 4. In step S1111, the download program 52-2 of a personal computer 1 receives the contents key which the key server 21-2 transmitted. The download program 52-2 decodes the received contents key with a key temporarily.

[0084] Step S1112 Setting, the IP communications program 13 of a personal computer 1 establishes the contents server 22-2 and IP communication link based on URL of the contents server 22-2 contained in the contents information acquired by processing of step S1106. In step S1501, the contents server 22-2 establishes a personal computer 1 and IP communication link.

[0085] In step S1113, the download program 52-2 of a personal computer 1 transmits the content ID acquired by processing of step S1106 to the contents server 22-2 through a communication network 4. In step S1502, the contents server 22-2 receives the content ID which the personal computer 1 transmitted. In step S1503, the contents server 22-2 reads the contents (enciphered) corresponding to the content ID which received at step S1502, and distributes them to a personal computer 1 through a communication network 4. In step S1114, the download program 52-2 of a personal computer 1 receives the contents which the contents server 22-2 transmitted.

[0086] Since processing of step S1115 thru/or step S1703 is the same as processing of step S115 thru/or step S703, the explanation is omitted.

[0087]

[Problem(s) to be Solved by the Invention] As mentioned above, since the procedures which supply contents and a contents key differ, respectively, when the server 5-1 which supplies contents and a contents key, or 5-2 asks for reception of a server 5-1 and the contents from 5-2, the download program 52-1 corresponding to a server 5-1 and the download program 52-2 corresponding to a server 5-2 are needed.

[0088] However, when a throughput, like there is little storage capacity with the small arithmetic proficiency of the equipment which receives contents is small, the equipment which receives contents cannot memorize two or more download programs, cannot switch a download program and cannot perform them.

[0089] This invention is made in view of such a situation, and it aims at enabling it to receive the contents and the key which are supplied in the procedure in which throughputs differ also with small equipment.

[0090]

[Means for Solving the Problem] 1st authentication means by which information offer equipment according to claim 1 attests the 1st information processor, The 2nd authentication means which attests the 2nd information processor or 3rd information processor, A reception-control means to control the reception of data which specifies the data which specify the 2nd information processor as the Request to Send of the contents and the key from the 1st information processor, and a list, or the 3rd information processor, When the data which specify the 2nd information processor are

received, in the procedure corresponding to the 2nd information processor While transmitting the Request to Send of contents and a key to the 2nd information processor When contents and a key are received from the 2nd information processor and the data which specify the 3rd information processor are received, in the procedure corresponding to the 3rd information processor While transmitting the Request to Send of contents and a key to the 3rd information processor It is characterized by including a communications control means to control a communication link to receive contents and a key from the 3rd information processor, and a transmission-control means to control the contents to the 1st information processor, and transmission of a key.

[0091] Information offer equipment establishes further a conversion means to transform either [at least] the coding method of contents, or the cipher systems into a predetermined coding method or a predetermined cipher system, and is made in things.

[0092] The 1st authentication step with which the information offer approach according to claim 3 attests the 1st information processor, The 2nd authentication step which attests the 2nd information processor or 3rd information processor, The reception-control step which controls the reception of data which specifies the data which specify the 2nd information processor as the Request to Send of the contents and the key from the 1st information processor, and a list, or the 3rd information processor, When the data which specify the 2nd information processor are received, in the procedure corresponding to the 2nd information processor While transmitting the Request to Send of contents and a key to the 2nd information processor When contents and a key are received from the 2nd information processor and the data which specify the 3rd information processor are received, in the procedure corresponding to the 3rd information processor While transmitting the Request to Send of contents and a key to the 3rd information processor It is characterized by including the communications control step which controls a communication link to receive contents and a key from the 3rd information processor, and the transmission-control step which controls the contents to the 1st information processor, and transmission of a key.

[0093] The program of a program storing medium according to claim 4 The 1st authentication step which attests the 1st information processor, and the 2nd authentication step which attests the 2nd information processor or 3rd information processor, The reception-control step which controls the reception of data which specifies the data which specify the 2nd information processor as the Request to Send of the contents and the key from the 1st information processor, and a list, or the 3rd information processor, When the data which specify the 2nd information processor are received, in the procedure corresponding to the 2nd information processor While transmitting the Request to Send of contents and a key to the 2nd information processor When contents and a key are received from the 2nd information processor and the data which specify the 3rd information processor are received, in the procedure corresponding to the 3rd information processor While transmitting the Request to Send of contents and a key to the 3rd information processor It is characterized by including the communications control step which controls a communication link to receive contents and a key from the 3rd information processor, and the transmission-control step which controls the contents to the 1st information processor, and transmission of a key.

[0094] An authentication means by which an information processor according to claim 5 attests the 1st information offer equipment, The contents to the 1st information offer equipment and the Request to Send of a key, the data that specify the 2nd information offer equipment which provides a list with contents and a key, And a transmission-control means to control transmission of either of the data which specifies the 3rd information offer equipment which offers contents and a key, It is characterized by including a reception-control means for the 1st information offer equipment to receive offer from the 2nd information offer equipment or the 3rd information offer equipment, and to control reception of the contents and the key which were transmitted.

[0095] The authentication step with which the information processing approach according to claim 6 attests the 1st information offer equipment, The contents to the 1st information offer equipment and the Request to Send of a key, the data that specify the 2nd information offer equipment which provides a list with contents and a key, And the transmission-control step which controls transmission of either of the data which specifies the 3rd information offer equipment which offers contents and a key, It is characterized by including the reception-control step which the 1st information offer equipment receives offer from the 2nd information offer equipment or the 3rd information offer equipment, and controls reception of the contents and the key which were transmitted.

[0096] The program of a program storing medium according to claim 7 The authentication step which attests the 1st information offer equipment, and the 1st information offer equipment, Contents and the Request to Send of a key, the data that specify the 2nd information offer equipment which provides a list with contents and a key, And the transmission-control step which controls transmission of either of the data which specifies the 3rd information offer equipment which offers contents and a key, It is characterized by including the reception-control step which the 1st information offer equipment receives offer from the 2nd information offer equipment or the 3rd information offer equipment, and controls reception of the contents and the key which were transmitted.

[0097] In information offer equipment according to claim 1, the information offer approach according to claim 3, and a program storing medium according to claim 4 The 1st information processor is attested and the 2nd information processor or 3rd information processor is attested. The reception of data which specifies the data which specify the 2nd information processor as the Request to Send of the contents and the key from the 1st information processor and a list, or the 3rd information processor is controlled. When the data which specify the 2nd information processor are received, in the procedure corresponding to the 2nd information processor While transmitting the Request to Send of contents and a key to the 2nd information processor When contents and a key are received from the 2nd information processor and the data which specify the 3rd information processor are received, in the procedure corresponding to the 3rd information processor While transmitting the Request to Send of contents and a key to the 3rd information processor, a communication link is controlled to receive contents and a key from the 3rd information processor, and the contents to the 1st information processor and transmission of a key are controlled.

[0098] In an information processor according to claim 5, the information processing approach according to claim 6, and a program storing medium according to claim 7 The

1st information offer equipment is attested. The contents to the 1st information offer equipment, and the Request to Send of a key, The data which specify the 2nd information offer equipment which provides a list with contents and a key, And transmission of either of the data which specifies the 3rd information offer equipment which offers contents and a key is controlled, the 1st information offer equipment receives offer from the 2nd information offer equipment or the 3rd information offer equipment, and reception of the contents and the key which were transmitted is controlled.

[0099]

[Embodiment of the Invention] Drawing 7 is drawing showing the gestalt of 1 operation of the digital data transmission system concerning this invention. The same number as the case of drawing 1 is given to the same part as the case of a configuration of that drawing 1 explained, and the explanation is omitted.

[0100] The portable media 3-1 are constituted possible [wearing], and the telephone one apparatus terminal 501 is connected to a communication network 4 by wireless. The telephone one apparatus terminal 501 downloads the contents (compressed and enciphered by the predetermined method) which received from the contents server 22-1 or 22-2 with the data of use conditions etc. through a communication network 4, and the portable media 3-1 equipped with contents and its use condition data are made to memorize it.

[0101] Based on the data of the use conditions relevant to contents, the telephone one apparatus terminal 501 is reproduced and outputs the contents memorized by the portable media 3-1 with which it is equipped to headphone or a loudspeaker etc. which is not illustrated. Walking around with the telephone one apparatus terminal 501, a user can download desired contents in a desired location, and can make the portable media 3-1 memorize the contents. A user can make the telephone one apparatus terminal 501 able to reproduce the contents memorized by the portable media 3-1, and can listen to the music corresponding to contents etc. by headphone etc.

[0102] The display operator guidance program 511 of the telephone one apparatus terminal 501 inputs directions of download etc., and makes LCM512 for clients perform processing corresponding to the directions while it displays the data (for example, a music name or use conditions etc.) relevant to contents. LCM512 for clients of the telephone one apparatus terminal 501 performs a series of processings (it mentions later) which download use condition data, contents, etc. in cooperation with LCM514 for servers of the substitute server 503.

[0103] LCM512 for clients of the telephone one apparatus terminal 501 consists of module groups which control to be able to use contents only on the use conditions which a copyright person specifies to each contents for the purpose of prevention of infringement of the copyright by unjust secondary use of contents. Playback conditions, copy conditions, migration conditions, or are recording conditions of contents etc. are included in use conditions.

[0104] LCM512 for clients attests whether the portable media 3-1 with which the telephone one apparatus terminal 501 is equipped are just, adds the data of the use conditions which the server 5 specified by the safe approach to contents (enciphered), and makes contents record on the portable media 3-1. With processing of migration of

contents etc., LCM512 for clients generates a required key, manages a key or controls the communication link with the portable media 3-1 connected.

[0105] The personal computer 502 is connected to the communication network 4. With cipher systems, such as DES, it enciphers and a personal computer 502 records them while changing into the method of predetermined compression the contents which received from the contents server 22-1 or 22-2, or were read in CD. A personal computer 502 records the data of use conditions in which the use conditions of contents are shown corresponding to the contents currently enciphered and recorded.

[0106] The display operator guidance program 11 of a personal computer 502 inputs directions of download or check-out etc., and makes LCM513 perform processing of the download corresponding to the directions, or check-out while it displays the data (for example, a music name or use conditions etc.) relevant to contents.

[0107] LCM513 of a personal computer 502 consists of module groups which control to be able to use contents only on the use conditions which a copyright person specifies to each contents for the purpose of prevention of infringement of the copyright by unjust secondary use of contents. Playback conditions, copy conditions, migration conditions, or are recording conditions of contents etc. are included in use conditions.

[0108] LCM513 attests whether the portable device 2 connected to the personal computer 502 is just, and performs processing of migration of contents etc. by the safe approach. With processing of migration of contents etc., LCM513 generates a required key, manages a key, enciphers contents or controls the communication link with the device connected.

[0109] Moreover, LCM513 checks the justification of the portable device 2. The portable device 2 checks the justification of the portable media 3-2, when equipped with the portable media 3-2. When the portable device 2 and the portable media 3-2 are just, LCM513 adds the data of the use conditions specified by a server 5 to contents (enciphered), and checks out contents to the portable media 3-2. The portable device 2 makes the portable media 3-2 with which it is equipped with the data relevant to contents memorize the contents by which the personal computer 502 was checked out.

[0110] LCM513 of a personal computer 502 checks out the contents currently enciphered and recorded to the portable device 2 connected. The portable device 2 makes the portable media 3-2 with which it is equipped with the data relevant to contents memorize the contents by which the personal computer 502 was checked out.

[0111] When the substitute server 503 can be used, LCM521 (it consists of the part or all the functions of LCM513) for PC of a personal computer 502 performs a series of processings which download use condition data, contents, etc. in cooperation with LCM514 for servers of the substitute server 503.

[0112] When the substitute server 503 cannot be used, LCM513 of a personal computer 502 performs processing of authentication with the same key server 21-1 or 21-2 [same] as LCM12 etc., and downloads use condition data, contents, etc.

[0113] The substitute server 503 performs processing of authentication with the key server 21-1 or 21-2 corresponding to the demand of the telephone one apparatus terminal 501 which performed and carried out mutual recognition of LCM514 for servers, or the personal computer 502 which carried out mutual recognition. The substitute server 503 supplies the contents key which received the contents key and was received from the key server 21-1 or 21-2 to the telephone one apparatus terminal 501 or a

personal computer 502 after processing of the key server 21-1 or the mutual recognition of 21-2. The substitute server 503 supplies the contents which received contents and received from the contents server 22-1 or 22-2 to the telephone one apparatus terminal 501 or a personal computer 502.

[0114] The substitute server 503 receives a contents key, after receiving contents from a server 5-1, when downloading contents and a contents key from a server 5-1. The substitute server 503 receives contents, after receiving a contents key, when downloading contents and a contents key from a server 5-2.

[0115] In any case, it is the same procedure (for example, contents are transmitted after transmitting a contents key), and the substitute server 503 supplies contents and a contents key for it to the telephone one apparatus terminal 501 or a personal computer 502, also when contents and a contents key are downloaded from a server 5-1, and also when contents and a contents key are downloaded from a server 5-2.

[0116] The telephone one apparatus terminal 501 or a personal computer 502 can receive contents and a contents key in the same procedure through the substitute server 503 by downloading contents and a contents key from a server 5-1 or 5-2.

[0117] Drawing 8 is drawing explaining the configuration of the telephone one apparatus terminal 501. CPU (CentralProcessing Unit)601 actually performs the various programs stored in ROM (Read-only Memory)602 or RAM (Random-Access Memory)603. ROM602 consists of an EEPROM (Electrically Erasable Programmable Read-Only Memory) or a flash memory, and, generally stores the data of immobilization fundamentally of the parameters the program which CPU601 uses, and for an operation. RAM603 consists of SRAM (Static RAM) etc., and stores a variable parameter suitably in the program used in activation of CPU601, and its activation.

[0118] The input section 605 is operated by the user, when it consists of an input key or a microphone and various kinds of commands are inputted into CPU601, or when inputting voice etc. A display 606 consists of a liquid crystal display etc., and displays various information in a text or an image.

[0119] The voice playback section 607 reproduces the contents memorized by the portable media 3-1 supplied from the data of a message partner's voice supplied from the communications department 608, or an interface 609, and outputs voice.

[0120] The communications department 608 connects with the public line network 31, stores in the packet of a predetermined method the data of a user's voice supplied from the data (for example, Request to Send of contents etc.) or the input section 605 supplied from CPU601, and transmits through the public line network 31. Moreover, the communications department 608 outputs the data (for example, contents etc.) stored in the packet which received, or the data of a message partner's voice to CPU601, RAM603, the voice playback section 607, or an interface 609 through the public line network 31.

[0121] It reads data, such as contents, from the portable media 3-1 with which it is equipped, and supplies them to CPU601, RAM603, or the voice playback section 607 while making the portable media 3-1 equipped with CPU601, RAM603, or the data supplied from the communications department 608 memorize an interface 609.

[0122] As for an interface 610, the external drive 631 is connected. Drive 631 reads the data or the program currently recorded on the magnetic disk 641 with which it is equipped, an optical disk 642 (CD-ROM is included), a magneto-optic disk 643, or

semiconductor memory 644, and supplies the data or program to ROM602 or RAM603 which are connected through the interface 610 and the bus 604.

[0123] CPU601 thru/or the interface 610 are mutually connected by the bus 604.

[0124] Drawing 9 is drawing explaining the configuration of the substitute server 503. CPU651 actually performs various application programs (for details, it mentions later) and OS (Operating System). Generally ROM652 stores the data of immobilization fundamentally of the parameters the program which CPU651 uses, and for an operation. RAM653 stores a variable parameter suitably in the program used in activation of CPU651, and its activation. These are mutually connected by the host bus 654 which consists of CPU buses etc.

[0125] The host bus 654 is connected to the external buses 656, such as a PCI (Peripheral Component Interconnect/Interface) bus, through the bridge 655.

[0126] A keyboard 658 is operated by the user when inputting various kinds of commands into CPU651. A pointing device 659 is operated by the user when performing the directions and selection of the point on the screen of a display 660. A display 660 consists of a liquid crystal display or CRT (Cathode Ray Tube), and displays various information in a text or an image. HDD (Hard Disk Drive)661 drives a hard disk, and records or reproduces the program and information which are performed by CPU651 to them.

[0127] Drive 662 reads the data or the program currently recorded on the magnetic disk 681 with which it is equipped, an optical disk 682, a magneto-optic disk 683, or semiconductor memory 684, and supplies the data or program to RAM653 with which it connects through the interface 657, the external bus 656, the bridge 655, and the host bus 654.

[0128] These keyboards 658 thru/or drives 662 is connected to the interface 657, and the interface 657 is connected to CPU651 through the external bus 656, the bridge 655, and the host bus 654.

[0129] The communications department 663 outputs the data (for example, content ID etc.) stored in the packet which received to CPU651, RAM653, or HDD661 through a communication network 4 while a communication network 4 is connected, and it stores in the packet of a predetermined method the data (for example, contents key etc.) supplied from CPU651 or HDD661 and transmits through a communication network 4.

[0130] The communications department 663 is connected to CPU651 through the external bus 656, the bridge 655, and the host bus 654.

[0131] Next, with reference to drawing 10, the configuration of the function of the digital data transmission system of this application is explained. The same number as the case of drawing 2 is given to the same part as the case of a configuration of that drawing 2 explained, and the explanation is omitted.

[0132] The telephone one apparatus terminal 501 performs the display operator guidance program 511, LCM512 for clients, the IP communications program 701, the ISP connection program 702, and the PHS/IMT communications program 703.

[0133] The PHS/IMT communications program 703 is a program for communicating through the public line network 31. The ISP connection program 702 is a program for connecting with ISP32. The IP communications program 701 is a program for including procedures, such as HTTP741 and Wap742, and communicating with the key server 21-1, the contents server 22-1, the shop server 23-1, the key server 21-2, the contents

server 22-2, the shop server 23-2, or the substitute server 503 through a communication network 4.

[0134] LCM512 for clients consists of a license manager 711, a download program 712, a format manager 713, etc.

[0135] The license manager 711 is a program for managing the use of contents based on the use conditions of contents, and consists of a use condition manager 721, a server authentication program 722, a PM authentication program 723, etc.

[0136] The use condition manager 721 makes the data of the use conditions which the portable media 3-1 have memorized to the portable media 3-1 update corresponding to playback of the contents which the portable media 3-1 have memorized etc. while performing management of whether playback of the contents which the portable media 3-1 have memorized etc. is permitted based on the use conditions of contents, or to forbid. The server authentication program 722 attests the substitute server 503 through a communication network 4. PM authentication program 723 attests the portable media 3-1, when the telephone one apparatus terminal 501 is equipped with the portable media 3-1.

[0137] The download program 712 consists of the key manager 724, a contents manager 725, a key information receiving agent 726, a contents information receiving agent 727, etc.

[0138] The key manager 724 receives a contents key from the substitute server 503, is made to run on contents, makes the portable media 3-1 memorize a contents key, and manages it. The key manager 724 contains the receiving agent 731 which receives a contents key from the substitute server 503.

[0139] The contents manager 725 receives contents (enciphered) with the use conditions of contents from the substitute server 503, and makes the portable media 3-1 memorize contents with the use conditions of contents. The receiving agent 732 of the contents manager 725 receives the use conditions of contents, and contents from the substitute server 503.

[0140] The key information receiving agent 726 receives URL which specifies the key server 21-1 which supplies the contents key corresponding to contents, or 21-2 from the shop server 23-1 or 23-2. The contents information receiving agent 727 receives URL which specifies the content ID which specifies desired contents and the contents server 22-1 which supplies desired contents, or 22-2 from the shop server 23-1 or 23-2.

[0141] The format manager 713 transforms into a predetermined method the coding method and cipher system of contents which were downloaded from the contents server 22-1 or 22-2 through the substitute server 503, respectively. The format manager 713 consists of a system discernment program 728, a format conversion program 729, etc.

[0142] The system discernment program 728 is a program for the download place of contents to identify whether it is a server 5-1 or it is a server 5-2. The format conversion program 729 changes the coding method and cipher system of contents.

[0143] Next, the configuration of the substitute server 503 is explained. The substitute server 503 performs LCM514 for servers, and the IP communications program 751.

[0144] LCM514 for servers contains the license manager 761, the sequence manager 762, etc.

[0145] The license manager 761 includes further the server authentication program 781 which attests the key server 21-1 or 21-2, PD authentication program 782 which attests the telephone one apparatus terminal 501.

[0146] The sequence manager 762 includes the key manager 771, the contents manager 772, the system discernment program 773, etc.

[0147] The key manager 771 includes the key distribution program 784 which distributes the contents key further received through the key receiving agent 783 which receives 21-2 to the key server 21-1 or a contents key through a communication network 4, and the communication network 4 to the telephone one apparatus terminal 501.

[0148] The contents manager 772 includes the contents distribution program 786 which distributes the contents which received further through the contents receiving agent 785 which receives 22-2 to the contents server 22-1 or contents through a communication network 4, and the communication network 4 to the telephone one apparatus terminal 501.

[0149] The system discernment program 773 is a program for the download place of contents to identify whether it is a server 5-1 or it is a server 5-2 based on the content ID supplied from the telephone one apparatus terminal 501.

[0150] The IP communications program 751 is a program for including procedures, such as HTTP787 and Wap788, and communicating with a server 5-1, 5-2, or the telephone one apparatus terminal 501 through a communication network 4.

[0151] Next, the telephone one apparatus terminal 501 explains the processing which downloads contents with reference to the flow chart of drawing 11 and drawing 12 from a server 5-1. In step S2101, the PHS/IMT communications program 703 of the telephone one apparatus terminal 501 establishes the public line network 31 and connection. In step S2201, the earth station which the public line network 31 does not illustrate establishes the telephone one apparatus terminal 501 and connection.

[0152] In step S2102, the ISP connection program 702 of the telephone one apparatus terminal 501 establishes ISP32 and connection through connection between the telephone one apparatus terminal 501 and the public line network 31. In step S2301, ISP32 establishes the telephone one apparatus terminal 501 and connection through connection between the telephone one apparatus terminal 501 and the public line network 31.

[0153] Processing with the subsequent telephone one apparatus terminals 501, and the key server 21-1, the contents server 22-1, the shop server 23-1 or the substitute server 503 is performed through connection between the telephone one apparatus terminal 501 and ISP32.

[0154] In step S2103, the IP communications program 701 of the telephone one apparatus terminal 501 establishes the shop server 23-1 and IP communication link. In step S2401, the IP communications program 124 of the shop server 23-1 establishes the telephone one apparatus terminal 501 and IP communication link.

[0155] In step S2402, the perusal program 123 of the shop server 23-1 transmits the digital data for perusal (for selection of contents) to the telephone one apparatus terminal 501 through a communication network 4. The browser program which the telephone one apparatus terminal 501 does not illustrate displays the text or image corresponding to the received digital data on a display 606, and a user is made to peruse it in step S2104. Moreover, by streaming playback of contents, the browser

program of the telephone one apparatus terminal 501 makes the voice playback section 607 reproduce contents, make a user try listening, or it makes the perusal program 123 of the shop server 23-1 search desired contents by the keyword, and displays the result on a display 606.

[0156] Processing of step S2402 and step S2104 is repeated until it determines the contents which a user purchases corresponding to a demand of the user of the telephone one apparatus terminal 501.

[0157] In step S2105, the browser program of the telephone one apparatus terminal 501 transmits a purchase request to the shop server 23-1 through a communication network 4. In step S2403, the perusal program 123 of the shop server 23-1 receives the purchase request transmitted from the telephone one apparatus terminal 501.

[0158] In step S2404, the contents information transmitting program 122 of the shop server 23-1 transmits the contents information containing the content ID for specifying URL of the contents server 22-1 which distributes contents, and contents corresponding to the purchase request which received by processing of step S2403 etc. to the telephone one apparatus terminal 501 through a communication network 4. In step S2106, the contents information receiving agent 727 of the telephone one apparatus terminal 501 receives the contents information which the shop server 23-1 transmitted.

[0159] In step S2405, the key information transmitting program 121 of the shop server 23-1 transmits key information, such as URL of the key server 21-1 which distributes the contents key of the contents corresponding to the purchase request which received by processing of step S2403, to the telephone one apparatus terminal 501 through a communication network 4. In step S2107, the key information receiving agent 726 of the telephone one apparatus terminal 501 receives the key information which the shop server 23-1 transmitted.

[0160] In step S2108, the IP communications program 701 of the telephone one apparatus terminal 501 establishes the substitute server 503 and IP communication link based on URL of the substitute server 503 currently recorded beforehand. In step S2501, the IP communications program 751 of the substitute server 503 establishes the telephone one apparatus terminal 501 and IP communication link.

[0161] In step S2109, the server authentication program 722 of the license manager 711 of the telephone one apparatus terminal 501 attests the substitute server 503. In step S2502, PD authentication program 782 of the license manager 761 of the substitute server 503 attests the telephone one apparatus terminal 501.

[0162] Processing of the mutual recognition of the telephone one apparatus terminal 501 and the substitute server 503 in step S2109 and step S2502 is processing of authentication of a challenge response method, and as compared with processing of the mutual recognition of the key server 21-1 and personal computer 1 in step S112 and step S602, there are few amounts of operations and it can be quickly performed also with little arithmetic proficiency or storage capacity. The telephone one apparatus terminal 501 and the substitute server 503 are the same operations, and generate and share a key from a response temporarily, respectively.

[0163] When processing of the authentication in step S2109 and step S2502 goes wrong, the processing to which the telephone one apparatus terminal 501 downloads contents is ended without downloading contents (when judged with the partner of authentication not being just).

[0164] In step S2110, the contents manager 725 of the telephone one apparatus terminal 501 transmits content ID to the substitute server 503. In step S2503, the substitute server 503 receives the content ID which the telephone one apparatus terminal 501 transmitted. In step S2111, the key manager 724 of the telephone one apparatus terminal 501 transmits the key information received by processing of step S2107 to the substitute server 503. In step S2504, the substitute server 503 receives the key information which the telephone one apparatus terminal 501 transmitted.

[0165] In step S2505, the system discernment program 773 of the substitute server 503 identifies that the download place of contents and a contents key is a server 5-1 based on the content ID which received by processing of step S2503.

[0166] In addition, the telephone one apparatus terminal 501 transmits URL of the contents server 22-1 with content ID, and you may make it the substitute server 503 receive URL of the contents server 22-1 with content ID in step S2503 in step S2110.

[0167] In step S2506, the IP communications program 751 of the substitute server 503 establishes the contents server 22-1 and IP communication link based on the result of discernment of processing of step S2505. In step S2601, the IP communications program 193 of the contents server 22-1 establishes the substitute server 503 and IP communication link.

[0168] In step S2507, the contents manager 772 of the substitute server 503 transmits the content ID acquired by processing of step S2503 to the contents server 22-1 through a communication network 4. In step S2602, the contents server 22-1 receives the content ID which the substitute server 503 transmitted. In step S2603, the contents distribution program 192 of the contents server 22-1 reads the contents (enciphered) corresponding to the content ID which received at step S2602 from the contents preservation program 191, and distributes them to the substitute server 503 through a communication network 4.

[0169] In step S2508, the receiving agent 785 of the contents manager 772 of the substitute server 503 receives the contents which the contents server 22-1 transmitted.

[0170] In step S2509, the IP communications program 751 of the substitute server 503 establishes the key server 21-1 and IP communication link based on the result of discernment of processing of step S2505. In step S2701, the IP communications program 155 of the key server 21-1 establishes the substitute server 503 and IP communication link.

[0171] In step S2510, the server authentication program 781 of the license manager 761 of the substitute server 503 attests the key server 21-1. In step S2702, the authentication program 151 of the key server 21-1 attests the substitute server 503.

[0172] For example, the master key KMSS is beforehand memorized by the key server 21-1, and ID of the individual key KPCC and the substitute server 503 is beforehand memorized by the substitute server 503. The master key KMCC is further memorized beforehand by the substitute server 503, and ID and the individual key KPSS of the key server 21-1 are memorized by the key server 21-1.

[0173] The key server 21-1 receives supply of ID of the substitute server 503 to the substitute server 503, applies a Hash Function to the master key KMSS which the ID and themselves have, and generates the same key as the individual key KPCC of the substitute server 503.

[0174] The substitute server 503 receives supply of ID of the key server 21-1 to the key server 21-1, applies a Hash Function to the master key KMCC which the ID and themselves have, and generates the same key as the individual key KPSS of the key server 21-1. A common individual key will be shared between doing in this way by both the substitute server 503 and the key server 21-1. A key is generated temporarily [still more temporary] using these individual keys.

[0175] Processing is ended when processing of the authentication in step S2510 or step S2702 goes wrong (when judged with the partner of authentication not being just).

[0176] In step S2511, the key manager 771 of the substitute server 503 transmits the content ID acquired by processing of step S2503 to the key server 21-1. In step S2703, the key server 21-1 receives the content ID which the substitute server 503 transmitted. In step S2704, the key distribution program 152 of the key server 21-1 reads the contents key which the key preservation program 153 matches with content ID, and is saved, and transmits the contents key (enciphered with the key temporarily which is shared between the key server 21-1 and the substitute server 503) to the substitute server 503 through a communication network 4. In step S2512, the key receiving agent 783 of the key manager 771 of the substitute server 503 receives the contents key which the key server 21-1 transmitted.

[0177] In step S2513, the key distribution program 784 of the key manager 771 of the substitute server 503 is enciphered with a key temporarily which decodes with a key the contents key received by processing of step S2512 temporarily which is shared between the key server 21-1 and the substitute server 503, and shares it between the telephone one apparatus terminal 501 and the substitute server 503, and the contents key enciphered is transmitted to the telephone one apparatus terminal 501 through a communication network 4. In step S2112, the receiving agent 731 of the key manager 724 of the telephone one apparatus terminal 501 receives the contents key which the substitute server 503 transmitted. The key manager 724 is decoded with a key temporarily which shares a contents key between the telephone one apparatus terminal 501 and the substitute server 503, is supplied to the key manager 102 of the portable media 3-1, and makes the key manager 102 memorize a contents key.

[0178] In step S2514, the contents distribution program 786 of the contents manager 772 of the substitute server 503 transmits the contents enciphered to the telephone one apparatus terminal 501 through a communication network 4. In step S2113, the receiving agent 732 of the contents manager 725 of the telephone one apparatus terminal 501 receives the contents which the substitute server 503 transmitted.

[0179] In step S2114, the PHS/IMT communications program 703 of the telephone one apparatus terminal 501 cuts connection with the public line network 31. In step S2202, the earth station which the public line network 31 does not illustrate cuts the telephone one apparatus terminal 501 and connection.

[0180] In step S2115, the format manager 713 of the telephone one apparatus terminal 501 changes a format of the contents which received by processing of step S2113. The contents manager 725 supplies the contents which changed the format to the portable media 3-1 through an interface 609, makes the contents manager 103 memorize contents, and ends processing.

[0181] Next, the telephone one apparatus terminal 501 explains the processing which downloads contents with reference to the flow chart of drawing 13 and drawing 14 from

a server 5-2. Processing of step S3101 thru/or step S3504 is performed by a server 5-2 and the list by the IP communications program 701, the ISP connection program 702, the PHS/IMT communications program 703, and the download program 712, and since it is the same as that of processing of step S2101 thru/or step S2504, the explanation is omitted, respectively.

[0182] In step S3505, the system discernment program 773 of the substitute server 503 identifies that the download place of contents and a contents key is a server 5-2 based on the content ID which received by processing of step S3503.

[0183] In step S3506, the IP communications program 751 of the substitute server 503 establishes the key server 21-2 and IP communication link based on the result of processing of discernment of step S3505. In step S3701, the key server 21-2 establishes the substitute server 503 and IP communication link.

[0184] In step S3507, the server authentication program 781 of the substitute server 503 attests the key server 21-2. In step S3702, the key server 21-2 attests the substitute server 503.

[0185] Processing of step S3507 and step S3702 is the same processing as processing of step S2510 and step S2702.

[0186] Processing is ended when processing of the authentication in step S3507 or step S3702 goes wrong (when judged with the partner of authentication not being just).

[0187] In step S3508, the key manager 771 of the substitute server 503 transmits the content ID acquired by processing of step S3503 to the key server 21-2. In step S3703, the key server 21-2 receives the content ID which the substitute server 503 transmitted. In step S3704, the key server 21-2 reads the contents key which matches with content ID and is saved, and transmits the contents key (enciphered with the key temporarily which is shared between the key server 21-2 and the substitute server 503) to the substitute server 503 through a communication network 4. In step S3509, the key receiving agent 783 of the key manager 771 of the substitute server 503 receives the contents key which the key server 21-2 transmitted.

[0188] In step S3510, the IP communications program 751 of the substitute server 503 establishes the contents server 22-2 and IP communication link based on the result of processing of discernment of step S3505. In step S3601, the contents server 22-2 establishes the substitute server 503 and IP communication link.

[0189] In step S3511, the contents manager 772 of the substitute server 503 transmits the content ID acquired by processing of step S3503 to the contents server 22-2 through a communication network 4. In step S3602, the contents server 22-2 receives the content ID which the substitute server 503 transmitted. In step S3603, the contents server 22-2 reads the contents (enciphered) corresponding to the content ID which received at step S3602, and distributes them to the substitute server 503 through a communication network 4.

[0190] In step S3512, the receiving agent 785 of the contents manager 772 of the substitute server 503 receives the contents which the contents server 22-2 transmitted.

[0191] Since processing of step S3512 thru/or step S3115 is the same as processing of step S2513 thru/or step S2115, the explanation is omitted.

[0192] As mentioned above, in any case, it is the same procedure (for example, contents are received after receiving a contents key), and the telephone one apparatus terminal 501 can receive contents and a contents key, also when downloading contents

and a contents key from a server 5-1 by minding the substitute server 503, and also when downloading contents and a contents key from a server 5-2.

[0193] Moreover, the procedure explained with reference to the flow chart of drawing 11 thru/or drawing 14 can shorten time amount which the telephone one apparatus terminal 501 has connected to the public line network 31 as compared with the processing (it explains with reference to the flow chart of drawing 16 and drawing 17) whose substitute server 503 mentioned later changes the coding method and cipher system of contents.

[0194] Next, with reference to drawing 15 , the configuration of other functions of the digital data transmission system of this application is explained. The same number as the case of drawing 10 is given to the same part as the case of a configuration of that drawing 10 explained, and the explanation is omitted.

[0195] The telephone one apparatus terminal 501 shown in drawing 15 does not have the format manager 713.

[0196] In addition to the license manager 761 and the sequence manager 762, LCM514 for servers of the substitute server 503 shown in drawing 15 contains the format manager 801.

[0197] The format manager 801 transforms into a predetermined method the coding method and cipher system of contents which were downloaded from the contents server 22-1 or 22-2, respectively. The format manager 801 consists of a system discernment program 811 and a format conversion program 812.

[0198] The system discernment program 811 is a program for the download place of contents to identify whether it is a server 5-1 or it is a server 5-2. The format conversion program 812 changes the coding method and cipher system of contents.

[0199] Next, the telephone one apparatus terminal 501 and the substitute server 503 which show the configuration explain to drawing 15 the processing which downloads contents with reference to the flow chart of drawing 16 and drawing 17 from a server 5-2.

[0200] Since processing of step S4101 thru/or step S4512 is the same as processing of step S3101 thru/or step S3512 respectively, the explanation is omitted.

[0201] In step S4512, the format manager 801 of the substitute server 503 changes a format of the contents which received by processing of step S4512.

[0202] In step S4514, the key distribution program 784 of the key manager 771 of the substitute server 503 is enciphered with a key temporarily which decodes with a key the contents key received by processing of step S4509 temporarily which is shared between the key server 21-2 and the substitute server 503, and shares it between the telephone one apparatus terminal 501 and the substitute server 503, and the contents key enciphered is transmitted to the telephone one apparatus terminal 501 through a communication network 4. In step S4112, the receiving agent 731 of the key manager 724 of the telephone one apparatus terminal 501 receives the contents key which the substitute server 503 transmitted. The key manager 724 is decoded with a key temporarily which shares a contents key between the telephone one apparatus terminal 501 and the substitute server 503, is supplied to the key manager 102 of the portable media 3-1, and makes the key manager 102 memorize a contents key.

[0203] In step S4515, the contents distribution program 786 of the contents manager 772 of the substitute server 503 transmits the contents enciphered to the telephone one apparatus terminal 501 through a communication network 4. In step S4113, the

receiving agent 732 of the contents manager 725 of the telephone one apparatus terminal 501 receives the contents which the substitute server 503 transmitted. The contents manager 725 supplies the contents (the format is changed) which received to the portable media 3-1 through an interface 609, and makes the contents manager 103 memorize contents.

[0204] In step S4114, the PHS/IMT communications program 703 of the telephone one apparatus terminal 501 cuts connection with the public line network 31. In step S4202, the earth station which the public line network 31 does not illustrate cuts the telephone one apparatus terminal 501 and connection, and processing is ended.

[0205] In addition, after the substitute server 503 receives contents from a server 5-1, the processing which receives contents and a contents key from a server 5-1 serves as the procedure of receiving a contents key from a server 5-1, and is performed similarly.

[0206] Thus, the substitute server 503 can change the coding method and cipher system of contents which were received from a server 5-1 or 5-2, and can also supply them to the telephone one apparatus terminal 501. In this case, it becomes unnecessary programming [which changes the coding method and cipher system of contents] the telephone one apparatus terminal 501. Therefore, the telephone one apparatus terminal 501 can perform processing which receives contents quickly also with smaller arithmetic proficiency or storage capacity as compared with the case where it is shown in drawing 10 .

[0207] Moreover, although it explained that contents were data of musical sound, the data of not only the data of musical sound but a static image, the data of a dynamic image, the data of a text, or a program may be used.

[0208] In addition, although the telephone one apparatus terminal 501 or the personal computer 502 explained that contents were downloaded, you may make it the telephone one apparatus terminal 501 or not only the personal computer 502 but a portable telephone, PDA (Personal DigitalAssistant), a digital video cassette recorder with an image pick-up function with communication facility, electronic notebook equipment with communication facility, or a pocket mold personal computer etc. download contents.

[0209] Moreover, although it explained that the telephone one apparatus terminal 501 communicated by PHS or IMT, you may make it communicate not only in PHS or IMT but in W-CDMA (Code Division Multiple Access), satellite communication, satellite broadcasting service, PSTN (Public Switched telephone network), xDSL (x Digital Subscriber Line) and ISDN (Integrated Services Digital Network), or a private network etc.

[0210] Although a series of processings mentioned above can also be performed by hardware, they can also be performed with software. When performing a series of processings with software, the program which constitutes the software is installed in a general-purpose personal computer etc. from a program storing medium possible [performing various kinds of functions] by installing the computer built into the hardware of dedication, or various kinds of programs.

[0211] The program storing medium which stores the program which is installed in a computer and made into the condition which can be performed by computer As shown in drawing 8 or drawing 9 , a magnetic disk 641 or a magnetic disk 681 (all contain a floppy disk), an optical disk 642 or an optical disk 682 (any -- CD-ROM (Compact Disc-Read Only Memory) --) DVD (Digital Versatile Disc) is included. A magneto-optic disk

643 or a magneto-optic disk 683 (all contain MD (Mini-Disc)), Or it is constituted by the package media which consist of semiconductor memory 644 or semiconductor memory 684, ROM602 in which a program is stored temporarily or permanently or ROM652, HDD661, etc. Storing of the program to a program storing medium is performed through the communications department 608 or the communications department 663 using the communication media of cables or wireless, such as a Local Area Network, the Internet, and digital satellite broadcasting, if needed.

[0212] In addition, in this specification, even if the processing serially performed in accordance with the sequence that the step which describes the program stored in a program storing medium was indicated is not of course necessarily processed serially, it is a juxtaposition thing also including the processing performed according to an individual.

[0213] Moreover, in this specification, a system expresses the whole equipment constituted by two or more equipments.

[0214]

[Effect of the Invention] According to information offer equipment according to claim 1, the information offer approach according to claim 3, and the program storing medium according to claim 4 The 1st information processor is attested and the 2nd information processor or 3rd information processor is attested. The reception of data which specifies the data which specify the 2nd information processor as the Request to Send of the contents and the key from the 1st information processor and a list, or the 3rd information processor is controlled. When the data which specify the 2nd information processor are received, in the procedure corresponding to the 2nd information processor While transmitting the Request to Send of contents and a key to the 2nd information processor When contents and a key are received from the 2nd information processor and the data which specify the 3rd information processor are received, in the procedure corresponding to the 3rd information processor While transmitting the Request to Send of contents and a key to the 3rd information processor Since a communication link is controlled to receive contents and a key from the 3rd information processor and the contents to the 1st information processor and transmission of a key were controlled The contents and the key which are supplied in the procedure in which the throughputs of the 1st information processor differ that it is small can be received now.

[0215] According to an information processor according to claim 5, the information processing approach according to claim 6, and the program storing medium according to claim 7 The 1st information offer equipment is attested. The contents to the 1st information offer equipment, and the Request to Send of a key, The data which specify the 2nd information offer equipment which provides a list with contents and a key, And transmission of either of the data which specifies the 3rd information offer equipment which offers contents and a key is controlled. Since the 1st information offer equipment receives offer from the 2nd information offer equipment or the 3rd information offer equipment and reception of the contents and the key which were transmitted was controlled, the contents and the key which are supplied in the procedure in which throughputs differ that it is small can be received.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1] It is drawing showing the configuration of the conventional digital data transmission system.

[Drawing 2] It is drawing showing the configuration of the function of the conventional digital data transmission system.

[Drawing 3] It is a flow chart explaining the conventional processing which a personal computer 1 downloads contents from a server 5-1, and checks out to the portable device 2.

[Drawing 4] It is a flow chart explaining the conventional processing which a personal computer 1 downloads contents from a server 5-1, and checks out to the portable device 2.

[Drawing 5] It is a flow chart explaining the conventional processing which a personal computer 1 downloads contents from a server 5-2, and checks out to the portable device 2.

[Drawing 6] It is a flow chart explaining the conventional processing which a personal computer 1 downloads contents from a server 5-2, and checks out to the portable device 2.

[Drawing 7] It is drawing showing the gestalt of 1 operation of the digital data transmission system concerning this invention.

[Drawing 8] It is drawing explaining the configuration of the telephone one apparatus terminal 501.

[Drawing 9] It is drawing explaining the configuration of the substitute server 503.

[Drawing 10] It is drawing explaining the configuration of the function of the digital data transmission system of this application.

[Drawing 11] The telephone one apparatus terminal 501 is a flow chart explaining the processing which downloads contents from a server 5-1.

[Drawing 12] The telephone one apparatus terminal 501 is a flow chart explaining the processing which downloads contents from a server 5-1.

[Drawing 13] The telephone one apparatus terminal 501 is a flow chart explaining the processing which downloads contents from a server 5-2.

[Drawing 14] The telephone one apparatus terminal 501 is a flow chart explaining the processing which downloads contents from a server 5-2.

[Drawing 15] It is drawing explaining the configuration of other functions of the digital data transmission system of this application.

[Drawing 16] The telephone one apparatus terminal 501 is a flow chart explaining the processing which downloads contents from a server 5-2.

[Drawing 17] The telephone one apparatus terminal 501 is a flow chart explaining the processing which downloads contents from a server 5-2.

[Description of Notations]

501 Telephone One Apparatus Terminal 503 substitute server 511 A display operator guidance program, 512 LCM for clients 514 LCM for servers, 601 CPU 602 ROM 603 RAM 608 communications department, 641 Magnetic disk 642 optical disk 643 A magneto-optic disk and 644 semiconductor memory 651 CPU 652 ROM 653 RAM 663 Communications department 681 Magnetic disk 682 An optical disk and 683 Magneto-optic disk 684 Semiconductor memory